控制系统隐私保护研究综述

王继民 [1, 2] 张纪峰 [3, 4] 陈嘉龙 [4]

摘 要 控制系统隐私保护是随着数字化、信息化和智能化的发展而诞生的新兴方向, 具有广泛的实际需求与应用价值, 是现代控制理论在新时代的重要发展. 鉴于此, 本综述从研究背景与意义、国内外现状、未来研究方向及总结与展望四个方面, 对该方向进行系统梳理. 控制系统隐私问题无处不在, 隐私保护对控制系统至关重要. 由于该方向具有交叉性、不确定性、实时性和应用性等特点, 其研究具有挑战性. 在国内外研究现状部分, 详细介绍基于系统结构的方法、基于确定性变换的方法和基于随机混淆或扰动的方法, 并着重阐述同态加密、安全多方计算、差分隐私等常见技术的理论基础及在控制系统中的应用. 针对面临的诸多挑战性问题, 总结未来重点研究方向, 尤其是隐私、控制与通信的一体化设计, 以及隐私保护与系统性能之间的权衡. 最后, 对该方向进行总结与展望, 旨在为相关研究人员提供参考, 进一步推动国家安全战略的实施.

关键词 隐私保护, 信息安全, 系统控制, 参数辨识, 分布式优化与博弈

引用格式 王继民, 张纪峰, 陈嘉龙. 控制系统隐私保护研究综述. 自动化学报, 2025, **51**(10): 2178−2200

DOI 10.16383/j.aas.c250082 **CSTR** 32138.14.j.aas.c250082

A Survey of Privacy Protection in Control Systems

WANG Ji-Min[1, 2] ZHANG Ji-Feng[3, 4] CHEN Jia-Long[4]

Abstract Privacy protection in control systems is an emerging research direction, arising with the development of digitalization, informatization, and intelligence. It has a wide range of practical needs and application value, representing an important development in modern control theory in the new era. In view of this, this review systematically surveys this direction from four aspects: Research background and significance, current research status both domestically and internationally, future research directions, and summary and outlook. Privacy issues in control systems are everywhere, privacy protection is critical to control systems. This direction is challenging due to its interdisciplinary nature, uncertainties, real-time requirements, and practical applications. In the current research status both domestically and internationally part, we provide a detailed introduction of the system structure-based method, the deterministic transformation-based method, and the stochastic obfuscation or perturbation-based method. In addition, we focus on elaborating the theoretical basis and applications in control systems of commonly used technologies, such as homomorphic encryption, secure multi-party computation, and differential privacy. In face of numerous challenging issues, we summarize key future research directions, especially the integrated design of privacy, control, and communication, as well as the trade-off between privacy protection and system performance. Finally, we provide a summary and an outlook for this direction, aiming to offer references for relevant researchers and further promote the implementation of national security strategies.

Key words Privacy protection, information security, systems control, parameter identification, distributed optimization and game theory

Citation Wang Ji-Min, Zhang Ji-Feng, Chen Jia-Long. A survey of privacy protection in control systems. *Acta Automatica Sinica*, 2025, **51**(10): 2178−2200

近年来, 网络安全越来越得到国家的重视. 一是国家战略层面, 习近平总书记在 2023 年 7 月全国网络安全和信息化工作会议与 2019 年 1 月 25 日十九届中央政治局第十二次集体学习中, 多次强调网络安全对国家安全和经济社会稳定运行的重要性, 特别是加强隐私保护. 二是社会民生层面,《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》[1] 提出加强涉及国家利

收稿日期 2025-03-06 录用日期 2025-05-29
Manuscript received March 6, 2025; accepted May 29, 2025
国家自然科学基金 (62433020, 62203045, T2293770) 资助
Supported by National Natural Science Foundation of China (62433020, 62203045, T2293770)
本文责任编委 段志生
Recommended by Associate Editor DUAN Zhi-Sheng

1. 北京科技大学自动化学院 北京 100083 2. 工业过程知识自动化教育部重点实验室 北京 100083 3. 中原工学院自动化与电气工程学院 郑州 450007 4. 中国科学院数学与系统科学研究院数学科学全国重点实验室 北京 100190
1. School of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing 100083 2. Key Laboratory of Knowledge Automation for Industrial Processes, Ministry of Education, Beijing 100083 3. School of Automation and Electrical Engineering, Zhongyuan University of Technology, Zhengzhou 450007 4. State Key Laboratory of Mathematical Sciences, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190

益、商业秘密、个人隐私的数据保护, 提升数据安全保障水平, 建立健全数据安全治理体系. 三是法律法规层面, 国家分别于 2017 年 6 月 1 日、2021 年 9 月 1 日和 2021 年 11 月 1 日颁布实施了《网络安全法》[2]、《数据安全法》[3] 和《个人信息保护法》[4], 涉及敏感信息的处理规则、数据安全制度与保护义务等方面. 世界各国也陆续颁布相关法规来保护数据隐私, 例如美国发布了包括隐私保护技术的关键新兴技术清单 (2024 年) 和相关《隐私保护法案》[5], 欧盟颁布了《通用数据保护条例》[6] 等. 控制系统隐私保护积极响应国家网络安全重大战略需求, 对于保障个人隐私、数据安全与国家安全具有重要意义.

信息控制技术和人工智能技术在诸多实际系统, 如物联网[7−8]、云控制系统[9]、智能电网[10]、5G 网络[11] 等新兴领域中得到越来越多的应用. 下面以系统辨识和协同控制为例进行说明. 具体地说, 系统辨识是处理工程系统、社会系统、生物系统等实际系统中模型不确定性和参数不确定性的关键手段, 其核心思想是利用最小二乘法、回归分析等统计学方法和拟牛顿法、内点法等优化算法, 根据观测到的输入输出数据建立能够准确描述系统动态特性的数学模型, 从而实现对复杂系统中重要参数的有效辨识. 它是利用数学方法辅助实现经济的宏观微观调控、流行病预测与防治、气象预测、反导拦截等重要社会经济问题、国家安全问题和科学问题的有效手段. 例如, 实现反导拦截技术的关键问题之一是如何准确地预测来袭导弹的轨迹, 而导弹轨迹预测需要对导弹动态特性及制导规律的建模与实时分析, 后者可转化为系统辨识问题[12]; 新冠病毒等传染病防治的重要环节之一是利用传染病动力学模型预测传染病的爆发, 而传染病动力学模型中存在难以直接获得的参数, 此时需要通过辨识手段解决该问题; 大规模电池系统包含数以千计的电池模块, 对其进行实时描述需要利用系统辨识工具. 协同控制问题随着分布式系统的大量应用而备受关注, 它是调控分布式系统的关键手段. 例如, 无人机蜂群战术作为当前军事领域引人注目的一个重要技术, 其思想就是由大量简单的无人机个体, 基于信息技术和智能控制技术, 对群居生物的信息交互和分工协作进行编组模仿, 从而实现高度智能自主的协同作战; 另外, 在以“星链”为代表的卫星星座系统中, 如何避免卫星之间的相互碰撞以及利用多颗卫星协同观测共同目标等均是重要的协同控制问题. 这些技术的广泛应用有效地提升了实际系统的整体效能, 但也带来了隐私泄露问题.

控制系统隐私问题无处不在. 针对控制系统隐私问题, 列出以下部分相关应用进行说明.

• 云控制系统. 云控制系统中, 为优化工艺流程, 工厂需要将生产数据传输到第三方云服务器进行计算处理. 在此过程中, 攻击者会窃听生产参数信息以获取工厂的隐私工艺流程, 给工厂造成经济损失[13]. Sultangazin 等[14] 将此问题建模成线性二次最优控制问题, 并采用同构变换技术遮盖系统输入, 防止云服务器窃取工厂的隐私生产参数信息.

• 交通监控. 交通监控系统中, 为实时估计某一路段的车流量, 车载雷达将车辆的位置、速度等信息发送给监测中心. 在此过程中, 车辆的位置轨迹可能会泄露, 从而导致泄露驾驶员经常访问地点的详细信息, 例如住所和工作地点[15]. Le Ny 等[16] 将此问题描述成 Kalman 滤波问题, 并采用差分隐私技术保护车辆的位置信息.

• 新能源系统. 新能源系统中, 为优化充电导致的电网整体负载, 电动汽车需要分享各自的充电计划, 例如每天充电时间和充电量等. 在此过程中, 汽车厂商会窃取充电计划, 进而据此向车主定向发送骚扰广告[17]. Han 等[18] 将此问题建模成分布式约束优化问题, 并采用差分隐私技术保护车主的家庭活动.

• 社交网络. 社交网络中, 为完成讨论或者投票, 个人往往需要发表自己的观点或者看法等私人信息. 在此过程中, 这些反映了个人的思想、信仰、价值观等核心隐私的信息会泄露给不法分子, 从而会被用于诈骗、骚扰或其他非法活动[19]. Wang 等[20] 将此问题建模成符号网络上的二分趋同, 并采用差分隐私保护个人实时观点.

• 智慧医疗. 智慧医疗系统中, 为推断出医疗预测的回归模型, 医院之间需要相互交换包含病人医疗记录的数据. 在此过程中, 病人的医疗记录可能会发生隐私泄露[21]. 一旦发生泄漏, 可能会侵犯患者的个人隐私权, 导致患者的诊疗信息被滥用, 进而影响医疗安全和诊疗效果; 引发患者与医疗机构之间的法律纠纷, 给双方带来不必要的法律风险和损失. 谭建伟等[22] 将此问题建模成多方 ARX 系统协作辨识, 并采用 Paillier 密码体制保护敏感信息.

• 智能建筑. 智能建筑应用中, 为估计商业建筑室内 CO_2 浓度或者温度, 室内传感器需要将这些信息 (与建筑物居住人数密切相关) 传给监测中心. 在此过程中, 建筑物居住人数会泄露给竞争对手, 竞争对手可能利用这些信息来制定更有针对性的营销策略, 从而抢占市场份额, 导致商业利益受损. Nekouei 等[23] 将此建模成状态估计问题, 并采用模型随机化法保护敏感信息.

• 人脸识别. 人工智能应用中, 为得到高准确率的人脸识别模型, 某人脸识别公司收集了大量人脸数据, 将其分成若干份用于分布式训练人脸识别模型, 辅助抓获在逃通缉人员. 在此过程中, 竞争对手窃取人脸数据和模型参数后能以极小成本获得价格优势, 从而导致商业利益受损. Wang 等[24] 将此问题建模成分布式随机优化问题, 并利用差分隐私方法保护训练样本.

• 智能电网. 智能电网中, 为实现电网中的经济调度, 包含用电信息、设备状态等信息的数据需要实时分享. 在此过程中, 用户个人习惯和行为、用电信息、设备状态等敏感数据会发生泄露, 进而被用来窥探隐私、偷窃、诈骗或推销广告等[25]. Yan 等[26] 利用 Paillier 密码体制和分布式趋同算法, 解决了电网中的经济调度问题并保护了网络传输的信息.

• 低空经济. 低空经济中, 为实时估计无人机的状态, 无人机需要向基站传输包含位置信息的数据. 在此过程中, 无人机的位置信息会发生泄露[27]. Yan 等[28] 将此问题建模成状态估计问题, 并利用 Paillier 密码体制保护无人机的位置信息.

除此之外, 分布式学习[29]、边缘计算系统[30] 和分布式智能相机[31] 等相关应用中的隐私问题也应得到关注[1]. 总的来说, 控制系统关联的控制输入、状态、输出和动态参数在应用中有时是非常敏感的. 因此, 隐私保护对于现代控制系统至关重要.

控制系统隐私泄露的后果有时是无法承受的. 比如, 2010 年, 震网病毒 (Stuxnet) 入侵伊朗核浓缩基础设施, 获取历史运行信息, 并进行重放攻击欺骗监控系统, 致使伊朗离心机“被杀”, 伊朗核项目被大大推迟; 2021 年, “DarkSide”黑客团伙窃取美国最大燃油运输管道商 Colonial Pipeline 大量的 VPN 账户密码, 获得敏感数据, 向系统注入勒索病毒, 美国官方宣布 18 个州进入紧急状态, 最终导致东海岸大部分地区出现燃料短缺. 由此可见, 控制系统隐私保护刻不容缓.

为刻画控制系统隐私问题, 首先需要明确四个要素: 系统动态特性、攻击者 (敌手) 能力、敏感信息和公开信息. 系统动态特性决定了敏感信息与公开信息之间的关系, 在隐私保护机制的设计中起着非常重要的作用. 攻击者能力是指计算能力 (在时间和存储资源方面, 具有有限或者无限计算能力) 和攻击方式 (被动攻击者和主动攻击者). 被动攻击者又分半诚实的攻击者和窃听者两种类型. 半诚实的攻击者是指遵守规定协议但试图了解他人敏感信息的系统参与者, 而窃听者是指只在通信信道上进行窃听的外部参与者. 主动攻击者可以任意行动 (例如, 必要时改变传输信息) 来学习敏感信息. 而敏感信息和公开信息则分别描述了哪些信息是需要保护的, 哪些信息是对手可以获得的. Xie 等[32] 研究了分布式趋同中敏感信息泄露所需的最少公开信息量.

综合目前文献中控制系统隐私保护方法, Zhang 等[33] 给出控制系统隐私安全的一般性定义, 即, 在给定公开信息的情况下, 当且仅当攻击者不能区分敏感信息的真实值和其候选值时, 此时系统被称为隐私安全的. 一个敏感信息的候选值指这样一个量, 它与真实值对应着相同的公开信息. 对于一个给定的敏感信息, 其所有候选值组成的集合在下文中将简称为该敏感信息的候选集. 这是个深刻且具有启发性的定义, 并有助于定量刻画隐私保护的程度. 例如, 如果考虑候选值个数的多少, 可以利用候选集的维数来量化隐私安全性; 如果考虑执行这种区分过程的困难性, 可以引入计算安全和完全安全 (定义详见第 1.2 节), 并分别应用于具有有限计算能力和无限计算能力的攻击者. 针对攻击者有限计算能力, Duan 等[34] 研究了隐私和性能平衡问题. 如果考虑敏感信息与公开信息的对应关系, 可以引入信息论来度量隐私泄露情况, 如 Fisher 信息[35]、离散条件熵[36]、互信息[37] 和 Cramér-Rao 下界[38] 等. Nekouei 等[39] 使用信息论概念来衡量隐私, 回顾了估计和云控制中的隐私保护.

控制系统隐私保护本质上融合了信息论、自动控制、传感器网络、分布式信息处理等多项技术, 是一个新兴的交叉领域, 也是当前系统科学和信息科学发展中一个极其重要的前沿研究方向. 该研究方向涉及若干关键基本问题, 包括隐私保护与控制之间内在联系的建立、隐私保护与系统性能的平衡以及复杂网络中的隐私保护控制等, 具有如下四个重要特点:

1) 交叉性. 由于在系统控制过程中, 系统量测及传输的信息包含参与者的敏感信息, 需要将控制目标和隐私保护目标一体化设计, 展现了信息论与控制理论的交叉融合.

2) 不确定性. 包括外部不确定性和内部不确定性. 外部不确定性主要是指远程指令和不同参与者间的网络通讯受到网络攻击、通讯约束和环境不确定性的影响, 以及通讯网络的拓扑结构和权重参数会随时间发生改变; 内部不确定性主要是指系统的动力学演化受到网络攻击的干扰以及系统的动力学含有未知的结构或参数.

3) 实时性. 在系统控制中, 数据的实时性有利于提高控制效果. 然而, 数据的实时传输会导致隐

[1] 所列应用包括但不限于上述成果, 实际建模中可根据所需保护的敏感信息和实现的具体控制任务, 选择合适的隐私保护方法和控制模型

私问题. 因此, 在保证数据实时传输的同时也应保证数据隐私安全, 这对在控制系统中实施隐私保护技术提出了新的要求.

4) 应用性. 随着科学技术的进步和实际需求的提升, 智能电网、智能交通、传感器网络安全信息融合、无人飞行器安全自主编队控制、大规模数字网络分布式安全计算等实际系统的结构、工作环境和控制任务也越来越复杂, 对控制性能和安全性能, 特别是系统的自主性、智能性和隐私性的要求越来越高.

关于控制系统隐私保护, 国内外已有一些综述文章, 如计算机领域的隐私及其在分布式优化和线性动态系统上的应用[40]、基于密码学控制系统隐私保护[41−42]、多智能体系统隐私保护[43−44] 等. 本综述在现有综述基础上, 不限隐私保护方法和控制目标, 全面梳理控制系统隐私保护的国内外研究现状, 同时加入更多最新研究成果.

1　国内外研究现状

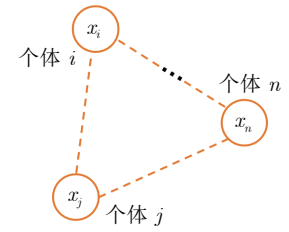
目前, 控制系统隐私保护理论及其应用研究已经成为各国政府、企业和科学界所关注的热点. 美国国家科学基金会 (NSF) 与英特尔 (Intel) 的联合基金已经累计资助 1 000 余项关于信息物理系统安全的研究. 欧盟地平线 2020 计划 (Horizon 2020) 也专门设有资助信息物理系统安全的项目. 谷歌、苹果、微软和华为等信息工业界巨头也纷纷加大对隐私保护算法的研究投入.

近年来, 国际学术界对控制系统隐私保护给予了高度关注. 例如文献 [45−51] 均指出控制系统隐私保护的重要性. 在近两届的控制界重要国际会议 IFAC World Congress 和 IEEE Conference on Decision and Control 上, 相关的成果不断涌现, 新问题、新思想、新技术层出不穷. 2020 年, 自动控制界三大期刊之一的 *IEEE Transactions on Automatic Control* 组织了有关分布式算法中隐私保护的专刊. 此外, *IEEE Transactions on Control of Network Systems*, *IEEE Transactions on Cybernetics*, *IEEE Transactions on Industrial Informatics*, *International Journal of Robust and Nonlinear Control* 等控制领域权威期刊也分别组织了该方向的专刊.

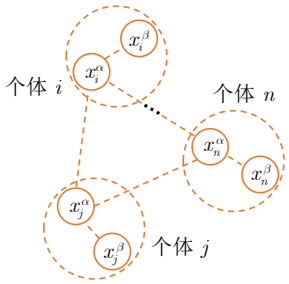
如何将现有的控制理论方法与隐私保护技术有机结合, 形成一体化分析与设计方法是控制系统隐私保护需要解决的一个基本科学问题, 目前已经取得了一批有价值的成果. 根据具体的研究方法, 可大致分为基于系统结构的方法、基于确定性变换的方法和基于随机混淆或扰动的方法.

1.1　基于系统结构的方法

该方法基于状态重构的标准能观性和输入再辨识的输入能观性. 所有可能的敏感信息的候选集构成了在标准加法运算下整个欧氏空间对不可观测子空间的商空间. 不可观测子空间的维数或基数越大, 攻击者就越难识别出需要保护的敏感信息. 换言之, 通过将敏感信息空间中的多个元素映射到公开信息空间 (即所有可能的公开信息的集合) 中的一个元素来实现系统的隐私安全. 此方法主要是通过柔和地改变系统的结构, 使得系统不可观, 进而实现控制系统隐私保护. 在分布式系统中, 常见的方法有改变动力学结构[52](如事先设定拓扑结构)、增加或者减少边连接、网络增强和调整初始状态. 例如, 美国克莱姆森大学 Wang[53] 通过将每个个体的初始状态分解为两个子状态, 其中第二个子状态只与第一个子状态进行相互作用, 而对其他节点不可见 (见图 1), 这样就可以避免节点的状态信息泄露, 从而实现分布式趋同的隐私保护. 基于此方法, 分布式状态估计[54]、有向图分布式趋同[55]、DoS 攻击[56] 和欺骗攻击[57] 下分布式趋同等的隐私保护也得到了研究. 此外, 通过梯度混淆机制[58] 或改变优化参数[59], 实现了分布式优化的隐私保护. 通过网络增强技术[60], 将每个个体初始状态分配或拆分为增强状态, 实现了分布式趋同的隐私保护. 通过引入一定的偏移量保护初值[61], 在迭代过程中逐步克服偏移量对控制精度的影响, 实现了分布式趋同的隐私保护.



(a) 状态分解前
(a) Before state decomposition



(b) 状态分解后
(b) After state decomposition

图 1　状态分解示例

Fig. 1　An example of state decomposition

1.2 基于确定性变换的方法

该变换是从敏感信息空间到另一个数学空间的映射, 这个数学空间可以是同一个敏感信息空间. 隐私安全是通过防止对手知道使用的确切映射来实现的. 敏感信息的候选集是映射到相应公开信息的所有可能变换的原像. 从这个角度看, 攻击者重建敏感信息往往比确定使用哪种变换更难. 常用的方法包括同构 (线性或仿射) 变换、同态加密方案 (如 RSA、ElGamal 和 Paillier) 和时变变换, 相关文献综述见表 1. 美国加州大学 Sultangazin 等[14] 引入同构变换, 解决了云控制系统的隐私问题; 文献 [62−69] 都在此方向上做出了有意义的工作. 尽管一些加密方案, 如 Paillier 和 ElGamal, 可以通过选择不同的随机参数将一个明文转换 (加密) 为不同的密文, 但是反转换 (解密) 会将这些密文再次映射回相同的明文. 因此, 这些基于密码学的方法本质

表 1 基于确定性变换的方法

Table 1 The deterministic transformation-based method

方法类别	实现技术	应用场景	对应文献
同态加密	Paillier 密码体制	机器学习	[70]
		离散时间参数估计	[22, 71]
		离散时间分布式优化	[26, 72−77]
		离散时间分布式趋同	[78−82]
		离散时间线性系统协同控制	[62, 83−86]
		云控制系统	[87−90]
		离散时间线性系统状态估计	[28, 66, 91−93]
		联邦学习	[94]
		离散时间模型预测控制	[95]
	RSA 密码体制	离散时间非线性系统控制	[96]
		离散时间线性系统控制	[97]
		离散时间系统状态估计	[98]
	ElGamal 密码体制	离散时间线性系统协同控制	[99−100]
		离散时间分布式优化	[101]
	Learning With Errors 密码体制	离散时间线性系统控制	[41, 102]
		离散时间线性系统状态估计	[103]
		离散时间系统分布式最优控制	[104]
	全同态加密	联邦学习	[105]
		离散时间线性系统控制	[106]
安全多方计算	混淆电路	机器学习	[107−108]
		基因分析	[109−110]
	秘密分享	机器学习	[111−118]
		联邦学习	[119−121]
		基因分析	[122]
		线性方程组求解	[123−124]
		连续时间多项式控制	[125]
		离散时间模型预测控制	[126]
	隐私比较	离散时间系统 Kalman 滤波	[127]
其他变换	同构变换	离散时间线性二次最优控制	[14]
	仿射变换	离散时间分布式趋同	[52]
		离散时间系统状态估计	[54, 64−65]
		云控制系统	[67]
		连续时间分布式优化	[68]
		离散时间分布式最优控制	[69]
	时变变换	连续时间分布式趋同	[63]

上是确定性的.

密码学中两类常见的密码算法为对称密码算法 (单钥密码算法) 和非对称密码算法 (公钥密码算法)[128]. 对称密码算法中的加密密钥能从解密密钥中推导出来, 反过来也成立. 对称密码算法要求发送者和接收者在安全通信前商定一个密钥, 算法的安全性依赖于密钥, 因此密钥必须得到保护, 以防攻击者对消息进行加/解密. 此外, 密钥越长, 算法越安全, 但计算复杂度越高. 对称密码的优点在于效率高 (加/解密速度能达到数十兆每秒或更多)、算法简单、系统开销小, 适合加密大量数据. 对称密码虽有良好特性, 但也存在着明显缺陷: 一是进行安全通信前需要以安全方式进行密钥交换, 这一步骤在某种情况下是可行的, 但在某些情况下会非常困难, 甚至无法实现; 二是密码规模大, 例如, A 与 B 两人之间的密钥必须不同于 A 与 C 两人之间的密钥, 否则给 B 的消息的安全性就会受到威胁. 在有 1000 个用户的团体中, A 需要保持至少 1000 个密钥 (999 个密钥给其他用户, 1 个密钥留给自己). 对于该团体中的其他用户, 此种情况同样存在. 这样, 这个团体需要将近 50 万个不同的密钥. 推而广之, N 个用户的团体需要 $N(N-1)/2$ 个不同的密钥. 非对称密码算法中的加密密钥与解密密钥不同, 不能由其中一个密钥推导出另一个密钥. 对称和非对称密码算法的差异体现在对称密码算法的加密过程简单、加/解密速度快、密钥较短, 而非对称密码算法的加密过程复杂、加/解密速度慢、密钥较长.

需要指出的是基于密码学的方法通常需要大量的计算, 其他基于确定性变换的方法计算量小, 但只适用于特定的系统.

同态加密是一种经典的对称加密方法, 它允许对加密数据进行某些操作[129], 加密可以隐藏所有传输的数据, 使通信网络中的外部各方不会从获得的加密中得到新的信息. 同态加密方案可以使密文在不解密的情况下进行某些类似针对明文的算术运算 (如加法或乘法). 因此, 实际应用中, 它显示出巨大的潜力, 近年来已被广泛用于各种场景, 包括云计算[99]、物联网[105] 和图像处理[70]. 一般来说, 同态性可以分为两种: 加法同态性和乘法同态性, 分别意味着加法和乘法在密文上是可操作的. 本文把加密和解密运算分别记作 $\mathrm{Enc}(\cdot)$ 和 $\mathrm{Dec}(\cdot)$; $\gcd(\cdot,\cdot)$ 表示求最大公约数; mod 为模数运算; 对正整数 N, 欧拉函数 $\phi(N)$ 表示小于 N 且与 N 互质的正整数的个数; Z_N 表示模 N 加法群; Z_N^* 表示模 N 乘法群; m_1, $m_2 \in Z_N$ 表示明文.

- 加法同态性. $\mathrm{Dec}(\mathrm{Enc}(m_1)\times\mathrm{Enc}(m_2)) = m_1 + m_2 \mod N$, 即

$$\mathrm{Enc}(m_1+m_2) = \mathrm{Enc}(m_1)\times\mathrm{Enc}(m_2) \mod N \quad (1)$$

- 乘法同态性. $\mathrm{Enc}(m_1\times m_2) = \mathrm{Enc}(m_1)\times\mathrm{Enc}(m_2)$.

同态加密可以分为全同态加密和半同态加密, 全同态加密[130] 可以同时支持加法和乘法同态, 而半同态加密[131−133] 只能支持其中之一. Paillier[131] 是一种典型的加法同态加密方法, RSA[132] 和 ElGamal[133] 是典型的乘法同态加密方法.

为更好地了解同态加密, 尤其是半同态加密, 下面给出常用的 $(m,\ m)$-门限 Paillier 密码体制[131]. 该密码体制有 m 个子密钥, 且只有当 m 个子密钥所有者都同意解密时才能进行正确解密. 它包括密钥生成、私钥分配、加密和解密四步, 具体描述如下:

- 密钥生成. 生成器选取大整数 $N = pq$, 其中 $p = 2p'+1$, $q = 2q'+1$, p', q', p, q 均为素数, 且 $\gcd(N,\ \phi(N)) = \gcd(pq,\ (p-1)(q-1)) = 1$. 令 $M = p'q'$, 选择 $k_{\mathcal{P}}$ 和 e 满足 $k_{\mathcal{P}} = 0 \mod M$, $k_{\mathcal{P}}e = 1 \mod N$. 随机选择 $b \in Z_N^*$, 令 $g = (1+N)^e b^N \mod N^2$, 则公钥为 $(N,\ g)$, 私钥为 $k_{\mathcal{P}}$.

- 私钥分配. 生成器随机选取 $k_{\mathcal{P}_0}$, $k_{\mathcal{P}_1}$, $\cdots$, $k_{\mathcal{P}_{m-1}}$ 使得 $k_{\mathcal{P}} = k_{\mathcal{P}_0} + k_{\mathcal{P}_1} + \cdots + k_{\mathcal{P}_{m-1}} \mod NM$, 将 $k_{\mathcal{P}_i}$ 传递给参与者 $\mathcal{P}_i$ 作为其私钥, $i = 0,\ 1,\ \cdots,\ m-1$.

- 加密. 对于任意的明文 $m \in Z_N$, 加密者在 Z_N^* 中随机选取 $h \in Z_N^*$, 密文

$$c = \mathrm{Enc}(m) := g^m h^N \mod N^2$$

- 解密. 对于 $i = 0,\ 1,\ \cdots,\ m-1$, 参与者 $\mathcal{P}_i$ 计算 $c_i = c^{2k_{\mathcal{P}_i}} \mod N^2$, 则

$$m = \mathrm{Dec}(c) := \frac{\left(\prod_{i=0}^{m-1} c_i \mod N^2\right) - 1}{N} \times \frac{N+1}{2} \mod N$$

该门限密码体制与 Paillier 密码体制一样, 明文空间为 Z_N, 密文空间为 $Z_{N^2}^*$. 其加密安全性建立在“判定复合剩余类是困难的”假设上, 能够抵御选择密文攻击 (一种针对加密体制的强攻击方式)[128, 131, 134].

密钥生成阶段所用到的素数 p' 和 q' 满足 $2p'+1$ 和 $2q'+1$ 也是素数, 这样的 p' 和 q' 称为 Sophie Germain 素数; 相应地, $p = 2p'+1$ 和 $q = 2q'+1$ 称为安全素数. 此外, 当 p' 和 q' 以二进制表示且具有相同的表示长度时, 密钥生成阶段所需的要求 $\gcd(N,\ \phi(N)) = 1$ 会自动满足[128].

(m, m)-门限 Paillier 密码体制继承了 Paillier 密码体制的良好特性. 对任意的明文 m_1, $m_2 \in Z_N$, 有加法同态性和密文隐藏性. 密文隐藏性指的是: 设 $c = \mathrm{Enc}(m)$, 对任意 $h' \in Z_N^*$, 有 $\mathrm{Dec}(ch'^N \mod N^2) = m$, 即 $ch'^N \mod N^2$ 也是 m 的密文. 这意味着可以对密文进行任意修改但能保证解密结果不变, 这是由 Paillier 密码体制密文的不唯一性决定的[131].

利用整数加法与整数乘法的关系以及式 (1), 可以得到 Paillier 密码体制的如下伪乘法同态性: 设 m_1 和 m_2 为两个明文, 则

$$\mathrm{Enc}(m_1 \times m_2) = (\mathrm{Enc}(m_1))^{m_2} \mod N^2 = (\mathrm{Enc}(m_2))^{m_1} \mod N^2 \quad (2)$$

注意, 上式中 $\mathrm{Enc}(m_1 \times m_2)$ 并非完全由密文计算得出, 所以式 (2) 并不是真正的乘法同态特性.

同态加密引起了众多控制学者的广泛关注, 已成功用于控制系统隐私保护. 半同态加密的估计只需要几毫秒, 而全同态加密的估计需要几个小时. 因此, 半同态加密对于实时估计、控制、优化等来说更加实用. 目前控制系统隐私保护中最常见的半同态加密方法是 Paillier 密码体制. 基于此密码体制, Xu 等[71] 提出了一种针对一类系统辨识问题的隐私保护安全协议; 美国宾夕法尼亚州立大学 Lu 等[72] 研究了一类分布式优化的隐私保护; 美国克莱姆森大学 Ruan 等[78] 研究了无向图下分布式趋同的隐私保护; 塞浦路斯大学 Hadjicostis 等[79−80] 研究了有向图下分布式趋同的隐私保护; Kishida[81, 83] 研究了该密码体制和量化器结合的加密控制; Chen 等[73] 在微电网分布式经济调度算法中采用了该密码体制和量化器结合; Lin 等[84] 给出了一种安全非线性网络控制系统设计框架; Murguia 等[85] 研究了线性系统动态输出反馈加密控制, 并解决了数据在密文空间上溢和下溢问题; Zhang 等[74] 研究了基于交替方向乘子法的完全分布式优化隐私保护; Alexandru 等[75−76] 研究了基于云端多方参与的受限约束二次优化问题; Ristic 等[91] 提出了仅有测距传感器的安全定位滤波器, 同时保护了导航仪和传感器的隐私; Zhu 等[92] 研究了具有未知有界噪声的人工神经网络的安全状态估计问题, 确保了测量信息在受带宽限制的通信网络内的安全传输; Chen 等[77] 研究了微电网的安全分布式经济调度问题, 并对量化输出进行隐私保护; Shi 等[86] 提出了一个基于模型的自适应加密网络控制框架, 并利用事件触发策略节约通讯资源; Yan 等[28] 为无人机系统提出了一个针对窃听者的安全估计协议; Darup 等[87]、Naseri 等[88]、Stabile 等[89] 与 Xu 等[90] 研究了云控制系统与 Paillier 密码体制的结合.

其他半同态加密体制也被用来解决控制系统的隐私保护. 基于椭圆曲线 ElGamal, 赵中原等[101] 研究了隐私保护分布式优化算法. 基于 Learning With Errors 密码体制, Kim 等[102] 加密系统输入和输出, 并提出一种可以在无限时间范围内运行而无需解密或重置其内部状态的动态反馈控制器. Zhang 等[93] 提出一个基于混合同态加密的安全状态估计协议, 同时使用乘法和加法同态加密保护模型参数、测量值和估计值. Strässer 等[96] 将 RSA 密码系统视为非线性动力系统, 利用非线性系统中的 Koopman 理论, 将这些动力系统转化为高维空间, 并解析推导出等效的线性系统, 进而利用线性系统工具开展分析, 同时实现了隐私保护和稳定性; Fauser 等[97] 将 RSA 密码体制与离散时间线性系统相结合, 证明了系统的安全性和稳定性; Teranishi 等[100] 在加密控制框架中研究了既能实现所需控制性能又能防止窃听攻击的信息物理系统, 并提出了样本辨识复杂度和样本解密时间两个新概念. 前者建立了控制系统的动态特性与系统可辨识性水平之间的关系, 而后者显示了辨识的计算时间与密码系统的密钥长度之间的关系. 基于这两个概念, 为了防止在给定系统运行时间内以给定精度进行辨识, 提出一种设计最佳密钥长度的方法, 并设计了最优控制器以最大化控制性能和辨识难度. 此外, 还有同态加密与其他隐私保护方法的结合, 如与差分隐私结合, Tran 等[103] 提出了多区域传输电网系统中直流和交流模型的隐私保护状态估计协议; 与秘密共享结合, Shi 等[94] 提出一种隐私保护联邦学习方案.

需要注意的是, 同态加密只能对非负整数进行加密, 而实际中控制系统的输入输出信息往往是用实数表示的, 所以有必要将同态密码体制的明文空间扩展到实数 (包括负整数). 此外, 使用该方法需要注意在密文运算过程中出现的数据上溢和下溢问题. 为了避免此问题, 并且克服 Paillier 密码体制只能适用于非负整数的限制, 谭建伟等[22] 通过对正/负整数的合理编码, 将其同态特性扩展到了负整数. 基于此, 考虑参与者彼此不信任情形下系统参数的隐私安全合作辨识问题, 提出了基于门限 Paillier 加密体制的安全最小二乘算法, 并给出了算法正确加/解密所需的明文空间大小条件.

在密码学领域, 有专门能够在多方参与的场景中保护数据隐私的密码学技术, 即安全多方计算 (Secure multi-party computation, MPC)[2]. 它可实现多个参与方协同计算关于秘密数据的任意函数,

[2] 此处与控制系统中常见的模型预测控制 (Model predictive control, MPC) 不同

除函数输出外不泄漏任何其他秘密信息. 计算机学界在 20 世纪 80 年代提出了 MPC 的概念, 并给出了多种关于任意函数 MPC 协议的可行性设计方法[135−140], 这些设计方法构成了后续大部分 MPC 协议的基本框架. MPC 支持任意 (多项式时间) 函数计算, 具有许多实际应用, 包括: 隐私保护机器学习[107, 111−118]、联邦学习[119−121]、基因分析[109−110, 122]、求解线性方程组[123−124] 等.

MPC 协议需要满足隐私性和正确性两个基本安全属性. 隐私性保证协议除函数输出外没有泄漏任何秘密信息, 正确性保证输出是预先协商函数的计算结果 (而不是其他函数). 即使存在内部攻击者, 这两个安全性质仍需成立. 具体来说, n 个参与方 $P_1, \cdots, P_n$ 运行 MPC 协议输出 $f(x_1, \cdots, x_n)$, 其中 x_i 是参与方 P_i 的秘密输入, f 是预先协商的函数. 隐私性保证不诚实参与方只能获得输出 $f(x_1, \cdots, x_n)$, 而不会泄漏诚实参与方 P_i 的秘密输入 x_i 的任何信息; 正确性保证参与方获得的输出结果为 $f(x_1, \cdots, x_n)$, 而不是 $F(x_1, \cdots, x_n)$, 其中 $F \neq f$ 为任意其他函数.

目前, 在计算机领域, 主要有两种方法设计 MPC 协议, 一种为秘密分享 (Secret sharing) 方法, 另一种为混淆电路 (Garbled circuit) 方法. 其中第一种方法的基本思想来源于文献 [136−138], 而第二种方法的基本思想来源于文献 [135, 140]. 一般而言, 秘密分享方法具有较低的通信带宽, 但轮数复杂度为 $\mathrm{O}(d)$, 适用于低延迟网络 (例如局域网), 其中 d 表示电路深度; 混淆电路方法的轮数复杂度为 $\mathrm{O}(1)$, 但需要较高通信带宽, 适用于高延迟网络 (例如广域网). 由于控制系统的独特性, 基于同态加密的 MPC 也是控制系统隐私保护的常见方法, 如基于半同态和秘密分享的两方计算[125]、基于 Paillier 密码体制和 MPC 设计扩展 Kalman 滤波器[127].

根据攻击者 (敌手) 能力, MPC 有以下分类方式:

- 攻击者行为. 如果攻击者是半诚实的, 那么它必须按照规范说明运行协议, 但可以通过观察协议记录获取更多的信息. 恶意的攻击者能够运行任何攻击策略和发送任意消息来攻击协议. 半诚实攻击者也称被动攻击者, 恶意攻击者也称主动攻击者.
- 腐化数量. 令 t 表示腐化门限 (即不诚实参与方数量的上界), n 表示所有参与方的总数. 根据 t 与 n 的关系, 主要分为两种情况: 1) 不诚实方占大多数情况, 其中 $n/2 \leq t < n$(大部分 MPC 协议考虑 $t = n - 1$); 2) 诚实方占大多数情况, 其中 $t < n/2$ (即允许严格少于一半数量的参与方被攻击者腐化).
- 攻击者计算资源. 即使攻击者拥有无限计算能力, MPC 协议仍可保证安全的话, 则称该协议为完全安全的 (或无条件安全的). 完全安全协议需要假设大多数参与方是诚实的. 计算安全的 MPC 协议则假设攻击者具有概率多项式时间计算能力, 计算安全的 MPC 协议可在不诚实方占大多数情况下实现.
- 腐化策略. 如果攻击者需要在协议运行前确定腐化参与方的集合, 则称该攻击者是静态的. 自适应的攻击者能在协议运行过程中确定腐化哪些参与方. 目前, 高效的 MPC 协议设计主要考虑的是静态腐化, 而满足自适应腐化安全性的 MPC 协议通常效率较低.

由上可见, 根据攻击者的攻击能力, MPC 协议可分为多种类型, 相应地满足不同的安全性和效率. 上述分类也有助于更好地理解控制系统隐私保护中所涉及的攻击者能力. 由于本综述侧重于控制系统隐私保护, 关于更多密码学和安全多方计算知识不再赘述, 感兴趣的读者可参考文献 [128, 141−142].

MPC 也已被用来实现控制系统隐私保护. MPC 通常是基于前面讨论的同态加密、秘密共享和混淆电路两两结合使用的, 如半同态和秘密分享结合[125]、秘密分享和混淆电路结合[108]. MPC 不仅能实现基本的加法和乘法, 还支持更复杂的运算, 这使其在需要高级运算的控制系统隐私保护中得到了广泛应用. 例如, 它已被用于需要矩阵求逆和比较操作的扩展 Kalman 滤波器[127], 以及需要投影操作进行约束优化的“隐含”模型预测控制器的加密实现[95, 126].

需要指出的是, 如果加密控制器设计包括复杂的非线性函数时, 可以考虑基于全同态加密的方法或基于 MPC 的协议, 但此时会大量使用计算或通信资源. 对于因安全问题而不允许使用多个操作单元的应用, 使用半同态加密方法是合适的. 由此可见, 每个加密控制方案在选择其方法时都应该考虑其所需的操作类型、可用资源和适当的安全模型. 今后, 为更好地应用于控制系统隐私保护, 基于同态加密的方案应旨在克服有限操作的约束, 基于 MPC 的方案应该解决由于合谋或外部窃听而可能出现的安全问题. 同时, 减少 MPC 的通信开销也应是值得关注的问题.

1.3 基于随机混淆或扰动的方法

该方法给系统引入了随机性. 将敏感信息与公开信息之间的关系视为一个映射, 通过将精心设计的噪声乘到或加到其象空间或原象空间中的元素中来引入随机不确定性. 这样一来, 敏感信息与公开信息之间的对应关系就不再是确定性的. 这不仅扩展了与公开信息相对应的给定敏感信息的候选集,

而且为其赋予了某种概率, 从而减少了敏感信息与公开信息之间的互信息, 提高了系统的隐私安全性. 清华大学 Mo 等[143] 设计一种对系统初值产生隐私保护效果的分布式趋同算法, 给出了算法的收敛速度及对系统初值的保护水平. Huang 等[144] 研究了观测值带随机扰动的分布式系统趋同问题, 发现证明系统状态趋同的几乎处处收敛十分困难, 从而转向求解系统状态趋同的均方收敛性. 这表明随着随机性的引入, 系统的性能会降低, 同时算法收敛性的证明会变得更加困难. 因此, 在实际应用中, 在使用该技术时需要考虑四个关键问题: 在哪里引入扰动; 使用什么样的扰动; 能产生多大的隐私保护力度; 对系统性能带来什么影响. Zhang 等[145] 指出添加适量的噪声足以实现分布式趋同的隐私保护. 差分隐私 (Differential privacy) 是控制系统隐私保护常用的一种随机扰动方法, 下面介绍其概念、性质及研究现状.

差分隐私是 Dwork 等[146−147] 提出的一种隐私保护方法. 差分隐私最开始是一个密码学概念, 被用来防范差分密码分析 (Differential cryptanalysis) 攻击. 其中差分密码分析指的是攻击者已知若干有差异的明文对, 通过计算密文的差异, 找出差异分布的统计特征. 差分指的是明文差异与密文差异组成的差异对. 攻击者可以通过对系统的不同数据返回查询的差异, 来对数据库进行差分攻击, 从而获得数据库的敏感 (隐私) 信息. 下面给出关于差分攻击的例子.

例 1. 假设现在有张三前 3 个月工资 (100, 200, 300) 构成的数据库, 只能查询张三直到目前为止的平均工资. 刚开始查询发现, 他的平均工资是 200, 在张三拿到第 4 个月工资后再次查询, 发现他的平均工资为 300. 于是可以推测出张三第 4 个月的工资为 600.

攻击者通过前后两次查询, 对数据库获得了更多知识. 关键在于如何防止攻击者对数据库获得更多知识. 为了防御差分攻击, 对邻接数据添加随机扰动, 使输出模糊化, 此时攻击者很难对数据库更加详细地了解. 具体的解决方案为: 对 2 次查询结果 $q_1 = 200$, $q_2 = 300$ 分别添加均值为 0、方差为 $2(\frac{100}{0.3})^2$ 的拉普拉斯噪声 Y_i, 即 $Y_i \sim \text{Lap}(\frac{100}{0.3})$, 此时输出记作 M_1, M_2, 部分取值见表 2. 此时有 $\text{e}^{-0.3} \leq \frac{P(a \leq M_2 \leq b)}{P(a \leq M_1 \leq b)} \leq \text{e}^{0.3}$, $\forall\ -\infty < a < b < \infty$, 其中 $P(A)$ 表示事件 A 发生的概率.

为更好地给出差分隐私的定义, 首先给出汉明距离 (Hamming distance) 的定义. 汉明距离指的是两个等长字符串对应位置处不同字符的个数. 例如, 11 与 10 的汉明距离是 1.

表 2 添加扰动后的两次输出

Table 2 Two outputs after adding perturbation

	$P(150 \leq M_i < 250)$	$P(250 \leq M_i < 350)$
$i = 1$	0.139	0.116
$i = 2$	0.116	0.139

差分隐私定义: 对于随机算法 $M : \mathbf{R}^d \to \text{Range}(M)$, 若 x, $y \in \mathbf{R}^d$ 之间的汉明距离不超过 1, $\forall S \subseteq \text{Range}(M)$, 均有

$$P(M(x) \in S) \leq \text{e}^{\epsilon} P(M(y) \in S) + \delta \quad \epsilon,\ \delta \geq 0$$

则称随机算法 M 满足 $(\epsilon,\ \delta)$-差分隐私. 特别地, 若 $\delta = 0$, 则称算法满足 ϵ-差分隐私.

上述定义在实际使用时, 可以根据需要将汉明距离推广为更一般的邻接关系 $Adj(x,\ y)$. 如在例 1 中, 为保护张三第 4 个月的工资不被攻击者得到, 针对数据空间 $\mathbf{R}^4$ 中的数据 $D = (d_1,\ d_2,\ d_3,\ d_4)$, $D' = (d'_1,\ d'_2,\ d'_3,\ d'_4)$, 可以将邻接关系定义为

$$Adj(D,\ D') \iff d_i = d'_i,\ 1 \leq i \leq 3,\ |d_4 - d'_4| \leq 1\,000$$

由此可见, 例 1 中的 (100, 200, 300, 0) 与 (100, 200, 300, 600) 满足上面定义的邻接关系. 邻接关系刻画了攻击者在多大的范围内无法确定隐私信息.

此外, 当差分隐私定义中的隐私预算 (Privacy budget) ϵ 充分小时, 则可以得到 $|P(M(x) \in S) - P(M(y) \in S)| \leq \text{e}^{\epsilon} - 1 + \delta \approx \epsilon + \delta$. 可见, 隐私预算 ϵ 和 δ 的大小与隐私保护程度成反比, ϵ 和 δ 越小, 随机算法 M 处理邻接数据 x, y 得到的输出 $M(x)$, $M(y)$ 落在任意给定的同一个集合 S 上概率的差别越小. 如在例 1 中, 分别取隐私预算 ϵ 为 0.1、0.3 和 10, 添加扰动 $Y_i \sim \text{Lap}(\frac{100}{\epsilon})$, 两次不同的输出见表 3. 由表 3 可得, ϵ 越小, 两次不同的输出值越接近, 攻击者越不容易通过概率分布推测出原始输出的大小和取值范围.

差分隐私具有如下两个性质: 1) 后处理免疫性.

表 3 隐私预算 ϵ 为 0.1、0.3 和 10 时的两次输出

Table 3 Two outputs when ϵ is 0.1, 0.3, and 10

		$P(150 \leq M_i < 250)$	$P(250 \leq M_i < 350)$
$\epsilon = 0.1$	$i = 1$	0.048 7	0.045 3
	$i = 2$	0.045 3	0.048 7
$\epsilon = 0.3$	$i = 1$	0.139	0.116
	$i = 2$	0.116	0.139
$\epsilon = 10$	$i = 1$	0.993	0.007
	$i = 2$	0.007	0.993

设随机算法 M 满足 ϵ -差分隐私, 则对任意映射 f, 算法 $f(M)$ 仍保持 ϵ -差分隐私. 这表明对后处理具有免疫性, 简单来说, 在经过差分隐私后的数据上进行运算仍保持其差分隐私性. 需要说明的是, 映射 f 不能与隐私数据相关. 2) 适应组合性. 设定义域为 D, 值域为 Q_1 的随机算法 $M_1 : D \to Q_1$ 满足 ϵ_1 -差分隐私, 定义域为 $(D,\ Q_1)$、值域为 Q_2 的随机算法 $M_2 : (D,\ Q_1) \to Q_2$ 对任意 $y \in Q_1$ 都有 $M_2(\cdot,\ y)$ 满足 ϵ_2 -差分隐私, 则算法 $M(D) = M_2(D,\ M_1(D))$ 满足 $(\epsilon_1 + \epsilon_2)$ -差分隐私. 这表明多次调用隐私数据 D 会使隐私预算增加, 进一步拓展了差分隐私算法的适用范围, 如控制系统中的迭代算法.

差分隐私在数学上概念简单, 且后处理有免疫性和适应组合性, 已得到控制学者的广泛关注, 并已成功应用到控制系统隐私保护, 相关文献综述见表 4. 文献 [148−150] 分别研究了差分隐私分布式优化[148]、差分隐私中心式和分布式系统的平均趋同[149]、系统辨识中差分隐私效果与估计性能之间的权衡[150]; 文献 [16, 18, 151] 分别研究了差分隐私下的 Kalman 滤波[16]、基于电动汽车充电模型的差分隐私分布式约束优化[18]、人群中流行病学传播[151]; 文献 [152−156] 分别研究了多输入多输出系统 Kalman 滤波[152−153]、非线性观测[154]、区间观测[155] 及 LQG[156] 等差分隐私保护; Nozari 等[157−158] 研究了分布式凸优化问题损失函数的差分隐私保护[157]、差分隐私的分布式趋同[158]. Liang 等[159] 考虑了连续时间分布式趋同的隐私保护, 并设计了事件触发机制降低通信频率. Wang 等[160] 结合差分隐私和 Paillier 密码体制, 进而改善了收敛精度与隐私保护之间的权衡. 近期, 文献 [20, 24, 161−166] 针对差分隐私系统控制, 采用随机逼近算法, 得到了许多重要成果. 文献 [161−163] 分别研究了连续时间分布式异步系统的平均趋同并保护初值、差分隐私分布式参数估计和有向图分布式在线估计. 针对分布式随机聚合博弈中的隐私泄露问题, 文献 [164] 首次利用输入扰动法和输出扰动法, 提出两种差分隐私分布式算法来寻求随机聚合博弈的均衡点, 同时保护每个参与者的敏感信息. 文献 [20] 基于时变噪声, 提出随机逼近型隐私保护算法, 实现了算法的均方和几乎处处收敛, 且可实现无穷时间序列的隐私保护, 并进一步给出了不同类型的算法步长和隐私保护噪声参数下一致性分析的统一框架, 包括衰减的步长和常数的噪声参数、常数的步长和指数衰减的噪声参数、衰减的步长和递增的噪声参数. 文献 [24] 基于输出扰动和基于梯度扰动的差分隐私分布式随机优化算法, 通过可变样本大小的方法, 建立了具有无限次迭代的有限累积隐私预算的差分隐私, 通过适当地选择李雅普诺夫函数, 实现了几乎处处收敛和均方收敛. 在此基础上, 文献 [165−166] 分别考虑了量化通信下的差分隐私分布式非凸随机优化[165], 及基于梯度追踪的差分隐私分布式随机优化[166].

表 4 差分隐私方法

Table 4 Differential privacy method

应用场景	对应文献
离散时间分布式优化	[18, 47, 50, 148, 157, 165−173]
离散时间分布式趋同	[149, 158, 160, 174−178]
离散时间线性系统控制	[150, 179−183]
社交网络参数估计	[151]
离散时间系统 Kalman 滤波	[16, 152−153]
离散时间系统非线性观测器设计	[154]
离散时间系统区间观测器设计	[155]
离散时间系统线性二次 Gauss 控制	[156]
连续时间分布式趋同	[159, 161]
离散时间参数估计	[162−163, 184−186]
离散时间分布式聚合博弈	[164, 187]
离散时间线性系统状态估计	[188−189]
离散时间系统线性二次控制	[190]
机器学习	[191−192]
联邦学习	[193]
非线性不确定系统异常检测	[194]

除上述研究成果外, 控制系统中的差分隐私保护也引起众多研究者的关注. 例如, 在差分隐私分布式优化方面, Cao 等[47]、Wang 等[50]、Xuan 等[167]、Wang 等[168−169]、Liu 等[170]、Ding 等[171]、Chen 等[172] 都取得了不错的成果; 在差分隐私估计和辨识方面, Han 等[185]、Katewa 等[184]、Sandberg 等[188]、Yan 等[186] 都有一些成果; 在差分隐私趋同方面, Gao 等[174−175]、Chen 等[176]、He 等[177]、Fiore 等[178] 都取得了一些成果. 此外, 文献 [173, 190] 研究了差分隐私约束优化和差分隐私 LQ 控制; 文献 [191−193] 研究了隐私性能增强下的分布式学习和联邦学习; 文献 [179−180] 研究了差分隐私与系统输出反馈; Rostampour 等[194] 研究了差分隐私分布式非线性不确定系统的异常检测; Qin 等[195] 研究了多种差分隐私机制比较和最优选取; Ye 等[187] 研究了差分隐私聚合博弈; 文献 [181−183] 研究了线性系统控制与差分隐私结合.

控制系统其他隐私保护方法包括秘密共享、乱码电路和不经意传输协议. 从本质上讲, 其中有些方法可以看作是转换和混淆处理技术的结合. 实际上, 每种技术都在使用各自的方法来保证候选集的存在, 并尽可能地将其扩展. 基于系统结构的技术和基于变换的技术通常对系统的稳定性要求不高,

而随机混淆技术往往要求系统具有足够的稳定性来抑制扰动的影响.

以上是对三类方法的简要回顾. 注意到目前控制系统隐私保护的研究尚处在起步阶段, 虽取得了一系列进展, 但该问题具有交叉性、不确定性、实时性、应用性和多目标性等特点, 使得所取得的成果存在很大局限性, 其难点在于突破原有的针对单一目标的传统控制理论框架, 并在控制性能与隐私保护水平等多目标之间寻求平衡. 然而, 现有理论成果往往难以满足工程实际需求, 这严重阻碍了控制系统隐私保护等相关技术的产业化进程. 综合现有的研究成果、局限和实际需求, 可以预见控制系统隐私保护在未来的发展方向包括:

1) 将信息论、密码学与控制理论相结合, 综合考虑控制系统性能和隐私保护指标等多方面属性, 对于较一般的控制系统模型, 提出高效和全新的控制系统隐私保护一体化理论与方法.

2) 将网络安全理论与控制理论相结合, 建立一个基于网络攻击、网络约束、网络不确定性和隐私保护多重网络需求的复杂控制系统数学模型, 给出有效的复杂控制系统隐私保护安全控制策略和算法.

3) 将控制系统隐私保护理论应用于智能电网、车联网、复杂疾病建模、无人飞行器安全自主编队控制、大规模数字网络分布式安全计算等实际系统中, 建立普适性的理论体系.

综上所述, 控制系统隐私保护是当前网络化控制系统和多自主体系统研究的发展趋势, 也是当前社会信息技术发展中的一个重要问题. 该问题的解决对于保障个人隐私、数据安全, 完善法律法规与维护国家网络安全, 助力我国低空经济快速发展, 促进社会稳定与发展, 提高工业的自动化和信息化水平具有重要的意义.

2 未来研究内容

控制系统隐私保护虽然取得了一批有价值的成果, 但仍面临着诸多挑战, 尤其是隐私保护和系统性能多目标兼顾难、隐私保护和系统实际需求匹配难等基本科学难题. 结合国内外研究现状和挑战性问题, 可以预见在不久的将来, 控制系统隐私保护的研究主要包括但不限于如下几个内容.

2.1 隐私、控制与通信一体化设计

天基通信系统等大装置、大网络在完成控制任务时, 通常面临保护关键数据隐私、降低网络通信成本等多元需求, 因此亟待建立隐私、控制与通信一体化全链条技术体系. 控制任务中隐私保护和通信成本问题的研究发展可大致分为三个阶段: 第一阶段是分立发展, 该阶段发展了一系列分布式网络的隐私保护方法和通信压缩方法. 例如前述的差分隐私趋同算法[149]、同态加密趋同算法[79] 侧重算法的隐私保护能力, 未考虑通信成本问题; 而 Li 等[196] 提出的有限数据率下的趋同算法和 Dimarogonas 等[197] 提出的事件触发趋同算法则侧重通信成本, 未考虑隐私保护问题. 第二阶段是两两结合, 该阶段发展了一系列将隐私保护机制与通信压缩机制有机结合的控制算法[61, 73, 81, 83, 159, 175], 以同时满足控制任务中的隐私需求和通信需求. 注意到, 与文献 [73, 81, 83] 相比, 文献 [175] 中的拉普拉斯隐私噪声具有无界支撑集, 因此相应地将量化通信机制调整为无穷值动态量化机制, 这在一定程度上增加了通信成本. 第三阶段是一体化设计, 该阶段试图挖掘通信压缩机制中的信息安全资源, 从而实现隐私保护和通信压缩的一体化设计. 当前研究主要围绕无偏概率量化器展开. Lang 等[193] 注意到无偏概率量化器中包含均匀分布的随机激励信号, 因此仅需在其基础之上增加一个特殊分布的较低功率的隐私噪声, 就能够使得隐私噪声与激励信号共同形成一个拉普拉斯噪声, 从而实现 ϵ-差分隐私. 该方法借助量化器中的信息安全资源, 一定程度上减少了隐私噪声. 此外, 一系列研究通过扩展隐私保护指标来刻画随机量化器自身的隐私保护能力. 例如, Wang 等[50] 和 Liu 等[182] 证明了基于不额外引入隐私噪声的概率量化器可以实现 $(0, \delta)$-差分隐私; Lv 等[198] 则设计了一种基于概率相似性的隐私保护指标, 来刻画概率量化器的隐私保护能力. 除概率量化器外, Liu 等[182] 基于能观性刻画了确定性无穷值均匀量化器的隐私保护能力.

“分立发展”、“两两结合”、“一体化设计”的发展趋势符合隐私、控制、通信一体化全链条技术体系. 一体化设计的核心在于控制任务中的隐私保护问题和通信成本问题存在本质共性: 即使用最少信息量的通信信号完成控制任务. 然而, 当前隐私保护和通信压缩一体化设计依然处于初级阶段, 这体现在当前一体化算法的单一性. 除文献 [182] 利用确定性无穷值均匀量化器刻画隐私保护能力等少量工作外, 当前工作主要还是基于无偏概率量化器实现隐私保护和通信压缩的一体化设计. 然而概率量化器并不完美, 主要体现在有效性、隐私性和通信成本三个方面. 有效性方面, 概率量化器中引入了随机性, 相应算法难以达到如动态量化器下的分布式算法[196] 的指数收敛. 隐私性方面, 由于概率量化器带来的量化误差具有一致上界, 因此不引入额外

隐私噪声时难以实现 ϵ -差分隐私. 通信成本方面, 概率量化器具有无偏特性, 这注定了概率量化器的输出无法做到一致有界, 因而难以实现理论意义上的有限值量化; 现有工作中的概率量化器要么考虑无穷值量化[182], 要么在有穷值量化外还需要传递与状态变量范数上界相关的实数信息[50]. 为满足实际场景中的多元需求, 未来应考虑更丰富、更多样的隐私保护和通信压缩一体化设计. 例如, 如何设计具有隐私保护能力的动态量化机制, 如何在理论上刻画有限值量化器的隐私保护能力.

2.2 经典控制理论解决隐私保护和系统性能问题

现有控制系统隐私保护方法都会在增强隐私安全性的同时降低系统性能 (如基于密码学方法的量化误差和基于随机混淆处理方法引入的随机性), 这符合"鱼和熊掌不可兼得"的传统观念, 但通过适当的创新, 可以在看似冲突的多目标之间找到平衡点, 实现真正的双赢. 针对控制系统隐私保护, 亟待解决隐私保护与系统性能的平衡问题, 加强隐私安全不应该牺牲太多系统的原始性能, 文献 [199] 也指出了这一问题依然是具有极大挑战的科学问题. 因此, 需要进一步研究这些误差与系统性能, 特别是系统稳定性之间的关系, 以设计性能更好的隐私保护机制. 虽然有些学者尝试在现有隐私保护机制上改善隐私保护与系统性能的平衡, 但是由于隐私保护引入导致收敛的误差仍然存在. 比如, 文献 [160] 虽尝试改善了收敛精度与隐私保护之间的权衡, 但并未消除由差分隐私带来的收敛误差. 为在原有系统性能的基础上实现隐私保护, 未来的研究趋势之一是将该问题转化为经典控制理论问题, 从而利用传统控制理论方法进行解决. 比如 Strässer 等[96] 利用非线性系统中的 Koopman 理论分析基于 RSA 密码系统的隐私保护和稳定性问题; Teranishi 等[100] 利用系统辨识理论提出一种设计最佳密钥长度的方法, 并设计了最优控制器以最大化控制性能和辨识难度.

虽有一些工作利用经典控制理论解决了隐私保护和系统性能问题, 但仍处于起步阶段, 尚有很多问题亟待解决. 比如, 差分隐私通过添加随机噪声实现隐私保护, 对于多方参与的参数辨识问题, 采用差分隐私方法后, 系统变成了典型的 Errors-in-variables (EIV) 系统, 故可采用传统的 EIV 辨识技术同时实现辨识和隐私保护. 下面以差分隐私多方协作辨识转化为传统的 EIV 辨识技术为例进行说明, 考虑如下多参与者的多方参数辨识模型

$$\begin{aligned} y_{k+1} = {} & a_1 y_k + a_2 y_{k-1} + \cdots + a_p y_{k+1-p} + \\ & b_{1,\,1} u_{1,\,k} + b_{1,\,2} u_{1,\,k-1} + \cdots + \\ & b_{1,\,q_1} u_{1,\,k+1-q_1} + \\ & b_{2,\,1} u_{2,\,k} + b_{2,\,2} u_{2,\,k-1} + \cdots + \\ & b_{2,\,q_2} u_{2,\,k+1-q_2} + \\ & \vdots \\ & b_{m,\,1} u_{m,\,k} + b_{m,\,2} u_{m,\,k-1} + \cdots + \\ & b_{m,\,q_m} u_{m,\,k+1-q_m} + \\ & \omega_{k+1}, \quad \forall k \in \mathbf{N} \end{aligned} \tag{3}$$

其中, $p \in \mathbf{N}$, $q_i \in \mathbf{N}$, $i = 1, \cdots, m$ 为已知系统阶数; $a_j \in \mathbf{R}$, $b_{i,\,l} \in \mathbf{R}$, $l = 1, \cdots, q_i$, $j = 1, \cdots, p$, $i = 1, \cdots, m$ 为系统未知参数; $y_k \in \mathbf{R}$ 是参与者 $\mathcal{P}_0$ 在时刻 k 的系统输出, $u_{i,\,k} \in \mathbf{R}$, $i = 1, \cdots, m$ 是参与者 $\mathcal{P}_i$ 在时刻 k 的系统输入; $\omega_k \in \mathbf{R}$ 是系统在时刻 k 的量测噪声. 记

$$\begin{aligned} \theta = {} & [a_1, \cdots, a_p, b_{1,\,1}, \cdots, b_{1,\,q_1}, \cdots, \\ & b_{m,\,1}, \cdots, b_{m,\,q_m}]^{\mathrm{T}} \\ \varphi_k = {} & [y_k, \cdots, y_{k+1-p}, u_{1,\,k}, \cdots, u_{1,\,k+1-q_1}, \\ & \cdots, u_{m,\,k}, \cdots, u_{m,\,k+1-q_m}]^{\mathrm{T}} \end{aligned}$$

则系统 (3) 可简写为

$$y_{k+1} = \theta^{\mathrm{T}} \varphi_k + \omega_{k+1}, \quad \forall k \in \mathbf{N}$$

为了保护每个参与者的敏感信息 (y_k 和 $u_{i,\,k}$), 采用差分隐私法给 y_k 和 $u_{i,\,k}$ 分别加上相应大小的噪声, 此时系统变成了典型的 EIV 系统[200]. 故可采用 EIV 辨识技术实现无偏辨识, 同时保护每个参与者的敏感信息.

因此, 如何用更多的经典控制理论工具 (如鲁棒控制[201]、非线性系统[202] 和自适应控制[203] 等) 解决控制系统性能和隐私保护问题是未来研究内容的重要组成部分.

2.3 更多密码学工具在控制系统隐私保护上的应用

该部分内容主要包括但不限于提高现有基于密码学方法的效率、恶意和半诚实攻击者同时存在的密码学算法和抗量子密码等.

- 提高现有基于密码学方法的效率. 现有的研究多采用半同态公钥加密方案来实现控制系统隐私保护, 该方案计算量大、耗时长. 因此, 如何将现有算法进行优化, 设计高效的同态加密方案和保护隐私的外包计算机制是未来亟待解决的问题. 在数据加密/解密的处理效率方面, 对称加密算法 (如 DES、

AES 等) 通常优于非对称加密算法 (如 RSA、ECC 等). 因此, 在可能的情况下, 优先选择对称加密算法可以降低计算复杂度. 此外, 通过改进算法的实现细节, 如优化循环结构 (如重新加密[106])、减少不必要的计算 (如部分加密[98]) 等, 可以降低算法的计算复杂度. 也可以利用并行计算, 对于一些可以并行化的密码算法, 可以利用多核处理器或分布式计算系统来加速计算过程. 通过将计算任务分配给多个处理器或节点, 可以显著降低单个任务的计算复杂度. 量化后加密或许是一种可行的方案, 为了降低加密所带来的高成本、低效率、高时延, 利用动态编码–解码方案[196], 把要传输的信息转换为 1 比特, 可以将需要加密的明文数据变为只需要加密 1 比特数据, 通过减小加密明文和通信传输数据的大小来减少加密的成本, 从而实现高效加密下控制系统隐私保护.

• 恶意和半诚实攻击者同时存在的密码学算法. 目前密码学工具在控制系统隐私保护上的应用主要关注机密性问题. 然而, 这些密码学工具本质上是可塑的, 恶意攻击者可能会篡改密文 (即便它们无法直接得知底层明文). 因此, 需要额外的措施来确保数据的完整性. 在密码学领域, 有一些解决完整性的方法, 但尚未引起控制学者的关注. 例如, 在同态加密中, 同态认证技术通过同态签名附加到数据上, 有效的签名可以证明计算的正确执行, 并且可以进行验证, 从而确保数据的完整性[204]. 此外, 基于对称密钥的解决方案, 如同态消息认证代码, 也是一种可行的选择[205]. 但是, 与同态加密一样, 同态身份验证也面临计算复杂度高的问题 (部分原因是安全问题). 特别地, 随着计算复杂性的增加, 验证工作量和签名的大小也会增加. 另一种更高效的方法是可验证计算. 与之前的方法不同, 有效的签名或消息认证代码只能通过正确的计算获得, 而在可验证计算中, 云计算通过基于概率测试和加密原语的参数 π 来向客户端证明计算是正确执行的, 防止了作弊的可能性. 通过构造参数 π, 云计算能够验证计算过程, 从而证明有符号的输入属于计算输出. 另一种有前景的工具是零知识证明 (zk)[206]. 非交互式变体 (如 zk-SNARKs[207]) 因其计算和通信效率脱颖而出. 事实上, 许多其他的 zk 证明方案会产生较大的通信开销. zk 在 MPC 中同样有应用, 在这种场景下, 各方能够证明它们遵守了协议, 同时不会泄露私人输入. 在 MPC 中, 也有在半诚实协议基础上针对恶意敌手的专门协议, 可以确保数据的完整性. 比如, Chida 等[208] 和 Keller 等[209] 分别针对恶意方和诚实方占多数情况下, 提出了具有恶意安全保障的离线和在线阶段的最新协议. 需要注意的是, 许多恶意安全协议仍然基于 SPDZ 或其改编方案. 未来的研究趋势在于如何将上述密码学领域解决完整性的方案应用至控制系统隐私保护中.

• 其他密码学工具. 随着计算能力的不断提高, 尤其是量子计算机的出现, 传统的加密算法可能面临被破解的风险. 因此, 需要研究更高效、更安全的数据加密技术来保护隐私. 其他基于密码学的方法, 如格加密[210] 和函数加密[211−212], 为此提供了新的实现途径. 格密码学是一种基于数学格理论中的计算困难问题的密码学方法. Learning With Errors 和 Ring-Learning With Errors 就是常见的基于格中的计算困难问题, 这些问题在经典计算机和量子计算机上都被认为是困难的, 因此格密码能够抵抗量子计算攻击. 函数加密支持有限制的密钥特性, 使密钥持有者只能得到关于加密数据的特定函数的计算结果, 得不到关于数据的任何其他信息. 这些工具在控制系统隐私保护中有着广阔的前景.

2.4 复杂控制问题的隐私保护

该部分内容主要包括但不限于复杂系统辨识、复杂分布式优化控制系统、多重网络攻击下控制系统及云控制系统等复杂控制问题的隐私保护.

• 复杂系统辨识的隐私保护. 常用的系统辨识和估计算法, 如 ELS 算法、投影 LMS 算法等, 在辨识和估计过程中会产生数据的传输, 从而导致敏感信息的泄露. 因此, 无论是从线性系统到非线性系统, 还是从单体系统到多体系统, 都亟待构造高效的、快速的和最优的隐私保护系统辨识和估计方法. 隐私保护下状态和参数估计问题核心点在于: 保证隐私性的前提下, 实现状态和参数的快速、准确估计. 由于现有关于隐私保护系统辨识的工作较少, 下面以隐私保护下状态估计为例进行说明.

现有隐私保护下状态估计主要分为单传感器状态估计的隐私保护和多传感器融合估计的隐私保护两类. 针对单传感器状态估计的隐私问题, 现有文献 [16, 152−153, 213−214] 考虑了有限时域 $[0, T]$ 上的隐私保护. 与单传感器状态估计相比, 采用多源数据的多传感器融合估计提高了状态估计的精度和鲁棒性. 针对多传感器融合估计的隐私问题, 有了一些结论[186, 189, 215]. 然而, 当前隐私保护下状态估计问题仍处于起步阶段, 主要体现在: 1) 单传感器状态估计问题只能实现有限时域 $[0, T]$ 上的隐私保护, 不适用于无穷时间场景; 2) 现有工作通常采用的隐私指标, 例如差分隐私、加密等, 不能直接反映攻击者对于隐私信息的估计精度; 3) 现有工作所研

究的系统限于线性随机动态系统, 而实际系统可能是非线性的. 与此同时, 非线性的引入会显著增加隐私保护下状态估计问题的研究难度. 为此, 未来的研究趋势在于研究更复杂的系统以及提出新的隐私保护指标. 例如, 研究非线性随机动态系统的隐私保护问题, 并提出能够直接反映攻击者对于隐私信息估计精度的指标.

此外, 针对异步、异类、混杂等多源数据驱动、随机非平稳集值系统以及通讯受限情形下的分布式系统辨识与估计问题, 其隐私保护也应得到关注.

● 复杂分布式优化控制系统的隐私保护. 通过上述国内外研究现状, 不难发现现有的分布式优化控制隐私保护仍有发展空间, 主要体现在: 1) 现有分布式优化控制隐私保护仅考虑了简单拓扑或系统结构, 实际中, 拓扑图有可能是有向的、时变的、切换的或者是随机变换的; 2) 现有分布式优化与博弈的隐私保护算法大多仅考虑了目标函数是敏感的, 实际上, 除目标函数外, 约束集、拓扑结构等也可能是敏感信息; 3) 现有结果仅考虑了简单离线优化 (博弈) 问题, 实际上分布式在线优化 (博弈)、分布式动态优化 (博弈)、带约束分布式优化 (博弈)、分布式零和博弈、非合作博弈等广泛存在; 4) 目标函数可能是随机的、非凸的、非光滑的、非李普希兹的等更一般情形. 因此, 未来的研究趋势在于如何构造复杂分布式优化控制系统的隐私保护理论.

注意到现有的学习算法大多是基于分布式优化或博弈算法, 此外, 机器学习数据质量和标注问题可能会影响学习模型的准确性和可靠性, 如生物医学数据机器学习中存在数据质量和标注问题, 且通常具有高度的异质性和复杂性. 研究隐私保护下强化学习、机器学习、Q 学习、无监督学习等学习算法时需同时考虑学习数据自身的特性. 因此, 未来的研究趋势在于建立一套适用于学习的隐私保护理论.

● 多重网络攻击下控制系统的隐私保护. 网络环境下系统个体间信息交流容易受到各种网络攻击, 比如拒绝服务 (DoS)、重放、零动态和虚假数据注入等攻击. 攻击者可能是理智且主动的, 可以选择任何有效的策略进行恶意攻击, 同时保持不被发现. 如何对此类攻击者的攻击进行数学建模并设计相应的隐私保护策略值得进一步研究. 例如可以考虑基于博弈论的方法. 此外, 这些网络攻击将严重影响算法的运行效果, 降低系统效能, 甚至摧毁整个控制系统, 并与系统中存在的非线性、随机性、不确定性等产生高度耦合. 因此, 有必要研究网络攻击对隐私保护能力及系统性能的影响. 此方向有了初步的结果, 如传感器攻击对控制状态的隐私影响[216]、基于卡方检验的攻击检测和隐私保护的平衡问题[217−218] 等已被研究. 假设攻击者是拜占庭的且注入信号是随机噪声时, 分布式趋同[178]、分布式估计[163] 的安全和隐私保护也得到了研究. 此外, 密码学工具研究了弹性同态加密问题[97]. 多重网络攻击下控制系统的隐私保护仍处于起步阶段, 存在的问题及未来的研究趋势主要体现在: 1) 现有弹性优化策略大多针对简单一致性问题和几类特殊网络攻击假设, 不具有一般性且难以推广. 2) 未来可考虑引入数字签名、可信计算等更多种密码学技术以增强系统安全性; 在不牺牲安全级别的情况下将多个明文加密为单个密文, 减少网络上传输的密文量, 从而降低网络通信负载; 设计弹性同态加密算法使其不仅对加性攻击具有弹性, 而且对乘性攻击也具有弹性 (此部分内容可以与第 2.3 节中的恶意和半诚实攻击者同时存在的密码学算法结合起来进行研究). 3) 引入更多攻击检测方法 (如几何控制方法[219]、强化学习方法[220] 和时间回溯方法[221] 等), 也可考虑基于攻防对抗的隐私保护算法. 从“攻击者视角”探讨攻击能力对控制任务的影响, 从“防御者视角”构建弹性控制算法及其隐私保护方案, 分析其在完成控制任务、抵抗攻击和隐私保护中的效用.

● 云控制系统的隐私保护. 云控制系统是一种基于网络化控制系统的新兴的控制系统, 它通过将控制器计算外包到云服务器, 利用云服务器强大的数据存储和计算能力, 实现了对复杂控制问题的快速解决[9]. 然而, 云控制系统在将控制器计算外包到云服务器的同时也加剧了敏感信息泄露的风险. 被动攻击者可在通信信道中发起侧信道攻击窃取通信数据, 并从中推断出尽可能多的敏感信息[222]. 针对云控制系统的隐私, 相关的隐私保护方法已经被提出, 如同态加密[75−76, 82, 87−90, 95, 126]、差分隐私[173, 190]、同构变换[14]、仿射变换[67] 等.

虽然云控制系统的隐私保护已取得初步进展, 但仍存在诸多亟待解决的问题. 以同态加密为例, 现有工作存在以下几方面问题: 1) 缺少加密过程对系统性能的量化分析; 2) 在面对高度耦合和非线性系统控制问题时, 往往难以适用或效果不佳; 3) 在加/解密过程中需要大量的计算和通信开销, 这使得其难以应用于包含大规模高维数据的系统的实时控制; 4) 无法应对量子计算带来的安全威胁[9, 222]. 因此, 针对云控制系统的隐私保护, 未来的研究趋势可能包括以下几个方面: 1) 采用传输延迟和数据吞吐量等作为标准化性能指标, 并设计相应的基准测试集来评估不同加密方案的性能[223]; 2) 将零知识证明[206]、隐私比较[127] 等密码学技术与非线性控

制[202]、自适应控制[203] 等经典控制理论相结合, 以应对高度耦合和非线性系统的隐私保护需求, 此部分可以与第 2.2 节结合起来进行研究; 3) 设计高效且实时的隐私保护算法, 如通过外包计算[224], 以降低计算复杂度并提高实时性, 此部分可以与第 2.3 节中提高现有基于密码学方法的效率结合起来进行研究; 4) 将量子安全技术[225] 与云控制系统理论相结合, 以增强云控制系统对潜在量子计算攻击的隐私保护能力, 此部分可以与第 2.3 节中其他密码学工具结合起来进行研究.

2.5 探索与离散事件系统不透明性的联系

离散事件系统不透明性是指在离散事件系统中, 系统保证秘密信息不被外界入侵者获取的能力. 这里, "离散事件系统"是一个离散状态、事件驱动的动态系统, 其中状态间的演变取决于特定离散事件的发生. 这种系统具有状态空间是一个离散集和状态转换机制是事件驱动的这两大特性. 在离散事件系统中, 不透明性是一种重要的信息安全性质. 它描述了即使入侵者完全了解系统结构, 并且能观测到部分信息流传递过程, 但由于系统的某些行为或状态变化对入侵者来说是不透明的, 因此入侵者无法准确预测或确定系统的秘密行为是否已经发生. 这里的"秘密行为"通常定义为系统的状态或语言的子集, 是系统不希望被外界所知的信息.

离散事件系统不透明性主要可以分为当前状态不透明性、初始状态不透明性、初始和最终状态不透明性、K 步不透明性和无穷步不透明性[226]. 当前状态不透明性: 是指入侵者或外部观察者不能确定当前系统所处的状态是否为秘密状态. 在离散事件系统中, 当前状态的不透明性是一个重要的安全属性, 它确保了系统的当前状态不会被未经授权的观察者所推断出来. 初始状态不透明性: 如果观察者不能确定系统的初始状态是否是秘密状态, 则系统是初始状态不透明的. 这种不透明性关注的是系统启动或开始运行时的状态是否保密. 初始和最终状态不透明性: 是当前状态不透明性与初始状态不透明性的扩展. 在初始和最终状态不透明性中, 秘密状态是成对定义的, 即, 不仅关注系统的初始状态, 还关注系统在某个时间点或运行结束时的最终状态. K 步不透明性: 这是一种更为复杂的不透明性类型, 它涉及到系统在一定步数 (K 步) 内的状态演化. 如果观察者无法在确定的时间内 (K 步内) 推断出系统是否处于秘密状态, 则系统被认为是 K 步不透明的. 无穷步不透明性: 与 K 步不透明性相对, 无穷步不透明性关注的是在整个系统运行过程中, 观察者都无法推断出系统是否处于秘密状态.

此外, 根据秘密集的性质和观察者的观测能力, 还可以进一步细分不透明性的类型. 例如, 在基于标签 Petri 网的离散事件系统中, 还可以考虑语言不透明性, 即系统的输出 (事件序列) 是否泄露了秘密状态的信息. 总的来说, 离散事件系统的不透明性是一个多层次、多维度的概念, 它涵盖了系统的当前状态、初始状态、最终状态以及状态演化的多个方面. 这些不透明性类型在保护系统安全性和隐私性方面发挥着重要作用. 为实现离散事件系统的不透明性, 通常需要采取一系列的安全措施和技术手段, 如加密、访问控制、数据隐藏等. 这些措施旨在保护系统的秘密信息不被泄露给未经授权的入侵者. 离散事件系统不透明性取得了很多不错的成果, 本文仅给出部分最新成果, 如将初始状态、当前状态、K 步和无限步等四不透明性与线性系统的两个子空间 (弱不可观察子空间和弱不可构造子空间) 相连, 并给出在受约束和不受约束的状态和输入集下秘密状态不透明性的条件[227]; 插入函数研究无限步不透明度和 K 步不透明度[228]; 随机离散事件系统的无穷步和 K 步不透明度的验证[229]; 动态信息释放机制验证当前状态不透明度[230]; 基础可达性图检查 K 步不透明度和无限步不透明度[231]; 基于近似的 Q 学习考虑线性时不变系统的不透明性[232]; 针对无限步不透明度, 研究最佳隐私执行器的定性和定量综合[233]; 离散时间线性时不变系统的不透明性[234].

Lu 等[235] 指出基于不透明性的隐私目标是确保对手无法从观察中确定系统状态是否属于预定义的秘密集, 所谓的控制系统隐私保护的隐私目标是保护数据隐私, 以便对于任何目标的任意值, 对手从观测中对目标值的获得都有无限的不确定性. 虽然不透明性与隐私保护二者的隐私目标不同, 但它们都旨在保护敏感信息不被泄露, 从这个角度来看, 对于控制系统来说并不是相互独立的概念, 不应区别对待. An 等[54] 研究了分布式状态估计的不透明性, 针对具有不同窃听能力的入侵者模型, 提出两种不透明度增强算法. 根据窃听节点构造的结构矩阵的秩, 建立了确保秘密状态不透明的必要和充分条件. 虽有初步探讨, 但是针对更一般的控制问题, 如系统辨识、协同控制、分布式优化等, 鲜有相关研究成果, 值得进一步研究. 同时注意到编辑函数[236−240]、监督控制[241] 是解决离散事件系统不透明性常见的方法, 是否可以扩展至更一般的控制问题? 因此, 探讨离散事件系统不透明性和控制系统隐私保护之间的联系与区别也是未来的重要内容之一.

2.6 构建适用实际控制系统的隐私保护理论体系

虽然隐私保护理论在实际控制系统中已有了初步应用, 如微电网的负载分配[242]、多机器人编队控制[243]、分布式经济调度[68, 172] 等, 也包括前文中的相关应用, 但是实际控制系统的建模、所需实现的控制任务往往是复杂的. 此外, 所需保护的敏感数据和隐私保护方法是多样的. 这主要体现在系统参数、系统状态、优化的目标函数和约束集等都可能是需要保护的敏感信息, 密码学、差分隐私、改变系统结构、仿射变换和量化等都可作为一种隐私保护方法. 因此, 实际控制系统的隐私保护往往很复杂[244]. 下面以智能电网和智慧交通为例进行说明. 在智能电网中, 敏感数据涵盖了从电力生产、传输、分配到消费的各个环节, 包括用户的用电习惯、能源消耗模式、设备运行状态等. 这些数据对于电网的优化运行、故障诊断和预测维护等方面具有巨大的价值, 但同时也可能包含用户的个人隐私信息. 如果这些数据被泄漏, 将对用户隐私和电网安全造成严重威胁, 甚至可能导致电网安全威胁、经济损失、法律纠纷和社会信任危机等. 为解决此问题, 利用同态加密方案, 分布式趋同控制和状态估计[26, 73, 77] 已被研究. 未来的研究包括但不限于以下几个方面. 一是设计基于同态加密的更高效、更轻量的隐私保护方案, 保证系统的高效性和低延迟的在线实时响应[245]. 比如, 通过优化算法来降低计算复杂度、减小加密数据大小、扩展对更广泛操作的支持以及开发更高效的噪声管理技术. 此外, 新型同态隐私保护协议与轻量级高效通信数据聚合结合[246] 或许也是一种可行的方案. 二是探索如何在不依赖值得信赖的第三方的情况下提供安全高效的密钥管理和分发机制, 同时确保所有个体之间的安全通信. 三是智能电网所面临的攻击者越来越智能, 因此有必要研究更安全的隐私保护方案. 此部分内容可以与第 2.3 ~ 2.4 节的理论研究相结合. 在智慧交通中, 数据隐私涉及保护个人数据、位置信息和车辆信息等敏感信息以免遭未经授权的访问或泄露. 为解决此问题, 一些隐私保护方法, 如差分隐私[16]、改变系统结构[247]、仿射变换[69]、同态加密[104] 等已用于智慧交通系统. 除了数据隐私, 系统安全和物理安全等安全要求也不容忽视[248]. 系统安全侧重于保护智慧交通系统基础设施 (例如通信网络和控制系统) 免受网络攻击. 物理安全旨在防止对智慧交通系统资产 (例如车辆和路边基础设施) 的物理攻击. 为满足这些安全要求, 可以实施包括敏感数据加密、安全通信协议、入侵检测和预防系统以及物理访问控制等多项措施.

由此可见, 如何建立健全一套适用于实际系统的隐私保护理论体系是有必要的. 未来的方向包括但不限于以下几方面: 设计更精细的隐私保护方案来满足不同场景下的隐私保护需求; 结合人工智能等技术, 构建更智能的隐私保护系统来自动识别和处理隐私泄露风险; 协同设计隐私保护算法及其相应的软件和硬件实现, 提升系统的整体效能. 由于隐私保护方法的计算复杂性和及时性限制了其实际应用, 可以设计专用的硬件/软件来有效地实现隐私保护算法, 这有助于扩展工业应用、促进隐私安全的研究. 此外, 为隐私保护算法开发专用集成电路和专用函数库可能是未来的一个好选择.

3 总结与展望

本综述聚焦控制系统隐私保护问题, 全面探讨了现有的控制系统隐私保护方法, 指出了未来几个可能的重点研究内容. 通过上述总结, 不难发现控制系统隐私保护的发展离不开隐私保护理论本身的突破性进展. 而从控制系统隐私保护这个层面来说, 在看到已有成绩的同时, 提高效率、精度、隐私安全性和适用范围的困难依旧存在. 这些困难有些是隐私保护理论本身固有的性质, 如同态加密的效率有时会不满足控制系统实时性的要求、差分隐私引入随机性会降低系统的性能等; 有些是源于在控制系统上发展隐私保护理论导致的, 如基于系统结构的方法适用范围难以一般化. 尽管这些困难依旧是牵制这个领域发展的因素, 但控制系统隐私保护服务于现实系统、解决现实问题是学界的目标. 同时需要指出的是“天下没有免费的午餐”, 控制目标和隐私目标的同时实现总是要在某方面付出代价的, 正如密码学中的安全性往往以效率为代价[249]. 最后希望通过本文的介绍能够给对控制系统隐私保护有所关注的研究者和初学者提供一些帮助和启发. 希望通过广大学者们的共同努力, 使得控制系统隐私保护技术更快更好地服务于现实世界的系统. 为助于我国低空经济快速发展, 加快我国工业和国防的自动化、信息化进程, 保障个人隐私、数据安全与国家网络安全作出贡献.

References

1 The State Council of the People′s Republic of China. Outline of the People′s Republic of China 14th five-year plan for national economic and social development and long-range objectives for 2035 [Online], available: http://www.ndrc.gov.cn/xxgk/zcfb/ghwb/202103/t20210323_1270124.html, July 11, 2025
(中华人民共和国中央人民政府. 中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要 [Online], available: http://www.ndrc.gov.cn/xxgk/zcfb/ghwb/202103/t20210323_1270124.html, 2025-07-11)

2 The National People′s Congress. Cybersecurity law of the Peo-

ple′s Republic of China [Online], available: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm, July 11, 2025
(全国人民代表大会. 中华人民共和国网络安全法 [Online], available: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm, 2025-07-11)

3 The National People′s Congress. Data security law of the People′s Republic of China [Online], available: http://www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html, July 11, 2025
(全国人民代表大会. 中华人民共和国数据安全法 [Online], available: http://www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html, 2025-07-11)

4 The National People′s Congress. Personal information protection law of the People′s Republic of China [Online], available: http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html, July 11, 2025
(全国人民代表大会. 中华人民共和国个人信息保护法 [Online], available: http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313088.html, 2025-07-11)

5 The United States Congress. The American privacy rights act [Online], available: http://www.congress.gov/crs-product/LSB11161, July 11, 2025

6 The European Parliament and of The Council. General data protection regulation (GDPR) [Online], available: http://gdpr-info.eu, July 11, 2025

7 Atzori L, Iera A, Morabito G. The internet of things: A survey. *Computer Networks*, 2010, **54**(15): 2787−2805

8 Chen Y K. Challenges and opportunities of internet of things. In: Proceedings of the 17th Asia and South Pacific Design Automation Conference. Sydney, Australia: IEEE, 2012. 383−388

9 Xia Y Q. Cloud control systems. *IEEE/CAA Journal of Automatica Sinica*, 2015, **2**(2): 134−142

10 Samad T, Annaswamy A M. Controls for smart grids: Architectures and applications. *Proceedings of the IEEE*, 2017, **105**(11): 2244−2261

11 Sufyan A, Khan K B, Khashan O A, Mir T, Mir U. From 5G to beyond 5G: A comprehensive survey of wireless network evolution, challenges, and promising technologies. *Electronics*, 2023, **12**(10): Article No. 2200

12 Wang Y H, Wang J, Fan S P. Parameter identification of a PN-guided incoming missile using an improved multiple-model mechanism. *IEEE Transactions on Aerospace and Electronic Systems*, 2023, **59**(5): 5888−5899

13 Gollmann D, Gurikov P, Isakov A, Krotofil M, Larsen J, Winnicki A. Cyber-physical systems security: Experimental analysis of a vinyl acetate monomer plant. In: Proceedings of the 1st ACM Workshop on Cyber-physical System Security. Singapore: ACM, 2015. 1−12

14 Sultangazin A, Tabuada P. Symmetries and isomorphisms for privacy in control over the cloud. *IEEE Transactions on Automatic Control*, 2021, **66**(2): 538−549

15 Eckhoff D, Sommer C. Driving for big data? Privacy concerns in vehicular networking. *IEEE Security & Privacy*, 2014, **12**(1): 77−79

16 Le Ny J, Pappas G J. Differentially private filtering. *IEEE Transactions on Automatic Control*, 2014, **59**(2): 341−354

17 Brighente A, Conti M, Donadel D, Poovendran R, Turrin F, Zhou J Y. Electric vehicles security and privacy: Challenges, solutions, and future needs. arXiv preprint arXiv: 2301.04587, 2023.

18 Han S, Topcu U, Pappas G J. Differentially private distributed constrained optimization. *IEEE Transactions on Automatic Control*, 2017, **62**(1): 50−64

19 Pham V V H, Yu S, Sood K, Cui L. Privacy issues in social networks and analysis: A comprehensive survey. *IET Networks*, 2018, **7**(2): 74−84

20 Wang J M, Ke J M, Zhang J F. Differentially private bipartite consensus over signed networks with time-varying noises. *IEEE Transactions on Automatic Control*, 2024, **69**(9): 5788−5803

21 Butler D. Data sharing threatens privacy. *Nature*, 2007, **449**(7163): 644−645

22 Tan Jian-Wei, Wang Ji-Min, Zhang Ji-Feng. Cooperative secure parameter identification of multi-participant ARX systems——A threshold Paillier cryptosystem-based least-squares identification algorithm. *Scientia Sinica Informationis*, 2023, **53**(12): 2472−2492
(谭建伟, 王继民, 张纪峰. 多方 ARX 系统的协作安全辨识——一种基于门限 Paillier 密码体制的最小二乘辨识方法. 中国科学: 信息科学, 2023, **53**(12): 2472−2492)

23 Nekouei E, Sandberg H, Skoglund M, Johansson K H. A model randomization approach to statistical parameter privacy. *IEEE Transactions on Automatic Control*, 2023, **68**(2): 839−850

24 Wang J M, Zhang J F. Differentially private distributed stochastic optimization with time-varying sample sizes. *IEEE Transactions on Automatic Control*, 2024, **69**(9): 6341−6348

25 Mo Y L, Kim T H J, Brancik K, Dickinson D, Lee H, Perrig A, et al. Cyber-physical security of a smart grid infrastructure. *Proceedings of the IEEE*, 2012, **100**(1): 195−209

26 Yan Y M, Chen Z Y, Varadharajan V, Hossain M J, Town G E. Distributed consensus-based economic dispatch in power grids using the Paillier cryptosystem. *IEEE Transactions on Smart Grid*, 2021, **12**(4): 3493−3502

27 Huang X. The small-drone revolution is coming——Scientists need to ensure it will be safe. *Nature*, 2025, **637**(8044): 29−30

28 Yan X H, Zhou G Z, Huang Y, Meng W, Nguyen A T, Huang H L. Secure estimation using partially homomorphic encryption for unmanned aerial systems in the presence of eavesdroppers. *IEEE Transactions on Intelligent Vehicles*, 2025, **10**(4): 2508−2518

29 Ma C, Li J, Wei K, Liu B, Ding M, Yuan L, et al. Trusted AI in multiagent systems: An overview of privacy and security for distributed learning. *Proceedings of the IEEE*, 2023, **111**(9): 1097−1132

30 Rao F Y, Bertino E. Privacy techniques for edge computing systems. *Proceedings of the IEEE*, 2019, **107**(8): 1632−1654

31 Serpanos D N, Papalambrou A. Security and privacy in distributed smart cameras. *Proceedings of the IEEE*, 2008, **96**(10): 1678−1687

32 Xie A T, Wang X F, Yang W, Cao M, Ren X Q. The least information set needed by privacy attackers. *IEEE Transactions on Automatic Control*, 2025, **70**(3): 1652−1666

33 Zhang J F, Tan J W, Wang J M. Privacy security in control systems. *Science China Information Sciences*, 2021, **64**(7): Article No. 176201

34 Duan X M, Xu Z, Yan R, Topcu U. Privacy-utility tradeoffs against limited adversaries. *IEEE Transactions on Automatic Control*, 2024, **69**(1): 519−526

35 Farokhi F, Sandberg H. Ensuring privacy with constrained additive noise by minimizing Fisher information. *Automatica*, 2019, **99**: 275−288

36 Nekouei E, Sandberg H, Skoglund M, Johansson K H. Optimal privacy-aware estimation. *IEEE Transactions on Automatic Control*, 2022, **67**(5): 2253−2266

37 Murguia C, Shames I, Farokhi F, Nešić D, Poor H V. On privacy of dynamical systems: An optimal probabilistic mapping approach. *IEEE Transactions on Information Forensics and Security*, 2021, **16**: 2608−2620

38 Guo L P, Wang J M, Zhao Y L, Zhang J F. State estimation with protecting exogenous inputs via Cramér-Rao lower bound approach. arXiv preprint arXiv: 2410.08756v2, 2025.

39 Nekouei E, Tanaka T, Skoglund M, Johansson K H. Information-theoretic approaches to privacy in estimation and control. *Annual Reviews in Control*, 2019, **47**: 412−422

40 Lu Y, Zhu M H. A control-theoretic perspective on cyber-phys-

ical privacy: Where data privacy meets dynamic systems. *Annual Reviews in Control*, 2019, **47**: 423−440

41 Kim J, Kim D, Song Y, Shim H, Sandberg H, Johansson K H. Comparison of encrypted control approaches and tutorial on dynamic systems using Learning With Errors-based homomorphic encryption. *Annual Reviews in Control*, 2022, **54**: 200−218

42 Schlüter N, Binfet P, Darup M S. A brief survey on encrypted control: From the first to the second generation and beyond. *Annual Reviews in Control*, 2023, **56**: Article No. 100913

43 Wang Y Q. Privacy in multi-agent systems. arXiv preprint arXiv: 2403.02631, 2024.

44 Chen Z Q, Wang Y Q. Privacy-preserving distributed optimization and learning. arXiv preprint arXiv: 2403.00157, 2024.

45 Sankar L, Rajagopalan S R, Mohajer S, Poor H V. Smart meter privacy: A theoretical framework. *IEEE Transactions on Smart Grid*, 2013, **4**(2): 837−846

46 Sankar L, Rajagopalan S R, Poor H V. Utility-privacy tradeoffs in databases: An information-theoretic approach. *IEEE Transactions on Information Forensics and Security*, 2013, **8**(6): 838−852

47 Cao X Y, Zhang J S, Poor H V, Tian Z. Differentially private ADMM for regularized consensus optimization. *IEEE Transactions on Automatic Control*, 2021, **66**(8): 3718−3725

48 Manshaei M H, Zhu Q Y, Alpcan T, Başar T, Hubaux J P. Game theory meets network security and privacy. *ACM Computing Surveys*, 2013, **45**(3): Article No. 25

49 Zhu Q Y, Başar T. Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Systems Magazine*, 2015, **35**(1): 46−65

50 Wang Y Q, Başar T. Quantization enabled privacy protection in decentralized stochastic optimization. *IEEE Transactions on Automatic Control*, 2023, **68**(7): 4038−4052

51 Guan Xiao-Hong, Shen Chao, Liu Ting. Data security is the foundation of cyberspace security. *China Cyberspace*, 2022, **1**: Article No. 233
(管晓宏, 沈超, 刘烃. 数据安全是网络空间安全的基础. 中国网信, 2022, **1**: Article No. 233)

52 Pan L L, Shao H B, Lu Y, Mesbahi M, Li D W, Xi Y G. Privacy-preserving average consensus via matrix-weighted inter-agent coupling. *Automatica*, 2025, **174**: Article No. 112094

53 Wang Y Q. Privacy-preserving average consensus via state decomposition. *IEEE Transactions on Automatic Control*, 2019, **64**(11): 4711−4716

54 An L W, Yang G H. Enhancement of opacity for distributed state estimation in cyber-physical systems. *Automatica*, 2022, **136**: Article No. 110087

55 Chen X M, Huang L Y, Ding K M, Dey S, Shi L. Privacy-preserving push-sum average consensus via state decomposition. *IEEE Transactions on Automatic Control*, 2023, **68**(12): 7974−7981

56 Hu Qin-Ling, Zheng Ning, Xu Ming, Wu Yi-Ming, He Xiong-Xiong. Privacy-preserving average consensus control for multi-agent systems under DoS attacks. *Acta Automatica Sinica*, 2022, **48**(8): 1961−1971
(胡沁伶, 郑宁, 徐明, 伍益明, 何熊熊. DoS 攻击下具备隐私保护的多智能体系统均值趋同控制. 自动化学报, 2022, **48**(8): 1961−1971)

57 Ying Chen-Duo, Wu Yi-Ming, Xu Ming, Zheng Ning, He Xiong-Xiong. Privacy-preserving average consensus control for multi-agent systems under deception attacks. *Acta Automatica Sinica*, 2023, **49**(2): 425−436
(应晨铎, 伍益明, 徐明, 郑宁, 何熊熊. 欺骗攻击下具备隐私保护的多智能体系统均值趋同控制. 自动化学报, 2023, **49**(2): 425−436)

58 Wang Y Q, Poor H V. Decentralized stochastic optimization with inherent privacy protection. *IEEE Transactions on Automatic Control*, 2023, **68**(4): 2293−2308

59 Gao H, Wang Y Q, Nedić A. Dynamics based privacy preservation in decentralized optimization. *Automatica*, 2023, **151**: Article No. 110878

60 Ramos G, Aguiar A P, Kar S, Pequito S. Privacy-preserving average consensus through network augmentation. *IEEE Transactions on Automatic Control*, 2024, **69**(10): 6907−6919

61 Rikos A I, Charalambous T, Johansson K H, Hadjicostis C N. Distributed event-triggered algorithms for finite-time privacy-preserving quantized average consensus. *IEEE Transactions on Control of Network Systems*, 2023, **10**(1): 38−50

62 Farokhi F, Shames I, Johansson K H. Private routing and ride-sharing using homomorphic encryption. *IET Cyber-physical Systems: Theory & Applications*, 2020, **5**(4): 311−320

63 Altafini C. A system-theoretic framework for privacy preservation in continuous-time multiagent dynamics. *Automatica*, 2020, **122**: Article No. 109253

64 Huang L Y, Leong A S, Quevedo D E, Shi L. Finite time encryption schedule in the presence of an eavesdropper with operation cost. In: Proceedings of the American Control Conference (ACC). Philadelphia, USA: IEEE, 2019. 4063−4068

65 Huang L Y, Ding K M, Leong A S, Quevedo D E, Shi L. Encryption scheduling for remote state estimation under an operation constraint. *Automatica*, 2021, **127**: Article No. 109537

66 Ni Y Q, Wu J F, Li L, Shi L. Multi-party dynamic state estimation that preserves data and model privacy. *IEEE Transactions on Information Forensics and Security*, 2021, **16**: 2288−2299

67 Zhang K X, Li Z J, Wang Y Q, Li N. Privacy-preserving nonlinear cloud-based model predictive control via affine masking. *Automatica*, 2025, **171**: Article No. 111939

68 Yun H, Shim H, Ahn H S. Initialization-free privacy-guaranteed distributed algorithm for economic dispatch problem. *Automatica*, 2019, **102**: 86−93

69 Zhao Y, Gong D K, Wen S X, Ding L, Guo G. A privacy-preserving-based distributed collaborative scheme for connected autonomous vehicles at multi-lane signal-free intersections. *IEEE Transactions on Intelligent Transportation Systems*, 2024, **25**(7): 6824−6835

70 Sultan A, Tahir S, Tahir H, Anwer T, Khan F, Rajarajan M, et al. A novel image-based homomorphic approach for preserving the privacy of autonomous vehicles connected to the cloud. *IEEE Transactions on Intelligent Transportation Systems*, 2022, **24**(2): 1936−1948

71 Xu C B, Zhao Y L, Zhang J F, Qi H S. System identification under information security. *IFAC-PapersOnLine*, 2017, **50**(1): 3756−3761

72 Lu Y, Zhu M H. Privacy preserving distributed optimization using homomorphic encryption. *Automatica*, 2018, **96**: 314−325

73 Chen W, Liu L, Liu G P. Privacy-preserving distributed economic dispatch of microgrids: A dynamic quantization-based consensus scheme with homomorphic encryption. *IEEE Transactions on Smart Grid*, 2023, **14**(1): 701−713

74 Zhang C L, Ahmad M, Wang Y Q. ADMM based privacy-preserving decentralized optimization. *IEEE Transactions on Information Forensics and Security*, 2019, **14**(3): 565−580

75 Alexandru A B, Gatsis K, Shoukry Y, Seshia S A, Tabuada P, Pappas G J. Cloud-based quadratic optimization with partially homomorphic encryption. *IEEE Transactions on Automatic Control*, 2021, **66**(5): 2357−2364

76 Alexandru A B, Gatsis K, Pappas G J. Privacy preserving cloud-based quadratic optimization. In: Proceedings of the 55th Annual Allerton Conference on Communication, Control, and Computing (Allerton). Monticello, USA: IEEE, 2017. 1168−1175

77 Chen W, Wang Z D, Ge Q B, Dong H L, Liu G P. Quantized distributed economic dispatch for microgrids: Paillier encryp-

tion-decryption scheme. *IEEE Transactions on Industrial Informatics*, 2024, **20**(4): 6552−6562

78 Ruan M H, Gao H, Wang Y Q. Secure and privacy-preserving consensus. *IEEE Transactions on Automatic Control*, 2019, **64**(10): 4035−4049

79 Hadjicostis C N. Privary preserving distributed average consensus via homomorphic encryption. In: Proceedings of the IEEE Conference on Decision and Control (CDC). Miami, USA: IEEE, 2018. 1258−1263

80 Hadjicostis C N, Domínguez-García A D. Privacy-preserving distributed averaging via homomorphically encrypted ratio consensus. *IEEE Transactions on Automatic Control*, 2020, **65**(9): 3887−3894

81 Kishida M. Encrypted average consensus with quantized control law. In: Proceedings of the IEEE Conference on Decision and Control (CDC). Miami, USA: IEEE, 2018. 5850−5856

82 Alexandru A B, Pappas G J. Private weighted sum aggregation. *IEEE Transactions on Control of Network Systems*, 2022, **9**(1): 219−230

83 Kishida M. Encrypted control system with quantiser. *IET Control Theory & Applications*, 2019, **13**(1): 146−151

84 Lin Y K, Farokhi F, Shames I, Nešić D. Secure control of nonlinear systems using semi-homomorphic encryption. In: Proceedings of the IEEE Conference on Decision and Control (CDC). Miami, USA: IEEE, 2018. 5002−5007

85 Murguia C, Farokhi F, Shames I. Secure and private implementation of dynamic controllers using semihomomorphic encryption. *IEEE Transactions on Automatic Control*, 2020, **65**(9): 3950−3957

86 Shi Y X, Nekouei E. Secure adaptive control of linear networked systems using Paillier encryption. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 2024, **71**(11): 5271−5284

87 Darup M S, Redder A, Shames I, Farokhi F, Quevedo D. Towards encrypted MPC for linear constrained systems. *IEEE Control Systems Letters*, 2018, **2**(2): 195−200

88 Naseri A M, Lucia W, Youssef A. Encrypted cloud-based set-theoretic model predictive control. *IEEE Control Systems Letters*, 2022, **6**: 3032−3037

89 Stabile F, Lucia W, Youssef A, Franzè G. A verifiable computing scheme for encrypted control systems. *IEEE Control Systems Letters*, 2024, **8**: 1096−1101

90 Xu K, Niu Y G, Zhang Z N. Cloud-based frequency control for multiarea power systems: Privacy preserving via homomorphic encryption. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2024, **54**(8): 5172−5184

91 Ristic M, Noack B, Hanebeck U D. Distributed range-only localization that preserves sensor and navigator privacies. *IEEE Transactions on Automatic Control*, 2023, **68**(12): 7151−7163

92 Zhu K Q, Wang Z D, Ding D R, Dong H L, Xu C Z. Secure state estimation for artificial neural networks with unknown-but-bounded noises: A homomorphic encryption scheme. *IEEE Transactions on Neural Networks and Learning Systems*, 2025, **36**(4): 6780−6791

93 Zhang Z Y, Cheng P, Wu J F, Chen J M. Secure state estimation using hybrid homomorphic encryption scheme. *IEEE Transactions on Control Systems Technology*, 2021, **29**(4): 1704−1720

94 Shi Z S, Yang Z Y, Hassan A, Li F G, Ding X Y. A privacy preserving federated learning scheme using homomorphic encryption and secret sharing. *Telecommunication Systems*, 2023, **82**(3): 419−433

95 Alexandru A B, Morari M, Pappas G J. Cloud-based MPC with encrypted data. In: Proceedings of the IEEE Conference on Decision and Control (CDC). Miami, USA: IEEE, 2018. 5014−5019

96 Strässer R, Schlor S, Allgöwer F. Decrypting nonlinearity: Koopman interpretation and analysis of cryptosystems. *Automatica*, 2025, **173**: Article No. 112022

97 Fauser M, Zhang P. A secure resilient homomorphic encryption scheme for control systems. *IEEE Transactions on Automatic Control*, 2025, **70**(6): 3711−3726

98 Zou L, Wang Z D, Shen B, Dong H L. Secure recursive state estimation of networked systems against eavesdropping: A partial-encryption-decryption method. *IEEE Transactions on Automatic Control*, 2025, **70**(6): 3681−3694

99 Darup M S, Alexandru A B, Quevedo D E, Pappas G J. Encrypted control for networked systems: An illustrative introduction and current challenges. *IEEE Control Systems Magazine*, 2021, **41**(3): 58−78

100 Teranishi K, Sadamoto T, Chakrabortty A, Kogiso K. Designing optimal key lengths and control laws for encrypted control systems based on sample identifying complexity and deciphering time. *IEEE Transactions on Automatic Control*, 2023, **68**(4): 2183−2198

101 Zhao Zhong-Yuan, Gao Wang, Jiang Lu-Yao, Ge Quan-Bo. Privacy-preserving distributed optimization algorithm based on elliptic curve ElGamal. *Acta Automatica Sinica*, 2025, **51**(1): 210−220
(赵中原, 高旺, 蒋璐瑶, 葛泉波. 基于椭圆曲线 ElGamal 的隐私保护分布式优化算法. 自动化学报, 2025, **51**(1): 210−220)

102 Kim J, Shim H, Han K. Dynamic controller that operates over homomorphically encrypted data for infinite time horizon. *IEEE Transactions on Automatic Control*, 2023, **68**(2): 660−672

103 Tran H Y, Hu J K, Pota H R. A privacy-preserving state estimation scheme for smart grids. *IEEE Transactions on Dependable and Secure Computing*, 2023, **20**(5): 3940−3956

104 He Y J, Chen Y, Pan C W, Ali I. Privacy-preserving distributed optimal control for vehicular platoon with quantization. *IEEE Transactions on Intelligent Transportation Systems*, 2024, **25**(10): 14572−14585

105 Hijazi N M, Aloqaily M, Guizani M, Ouni B, Karray F. Secure federated learning with fully homomorphic encryption for IoT communications. *IEEE Internet of Things Journal*, 2024, **11**(3): 4289−4300

106 Kim J. Further methods for encrypted linear dynamic controllers utilizing re-encryption. *IEEE Transactions on Automatic Control*, 2024, **69**(10): 6974−6979

107 Chandran N, Gupta D, Rastogi A, Sharma R, Tripathi S. EzPC: Programmable and efficient secure two-party computation for machine learning. In: Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P). Stockholm, Sweden: IEEE, 2019. 496−511

108 Tjell K, Schlüter N, Binfet P, Schulze Darup M. Secure learning-based MPC via garbled circuit. In: Proceedings of the 60th IEEE Conference on Decision and Control (CDC). Austin, USA: IEEE, 2021. 4907−4914

109 Jha S, Kruger L, Shmatikov V. Towards practical privacy for genomic computation. In: Proceedings of the IEEE Symposium on Security and Privacy (sp 2008). Oakland, USA: IEEE, 2008. 216−230

110 Jagadeesh K A, Wu D J, Birgmeier J A, Boneh D, Bejerano G. Deriving genomic diagnoses without revealing patient genomes. *Science*, 2017, **357**(6352): 692−695

111 Mohassel P, Zhang Y P. SecureML: A system for scalable privacy-preserving machine learning. In: Proceedings of the IEEE Symposium on Security and Privacy (SP). San Jose, USA: IEEE, 2017. 19−38

112 Mohassel P, Rindal P. ABY3: A mixed protocol framework for machine learning. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Toronto, Canada: Association for Computing Machinery, 2018. 35−52

113 Schoppmann P, Gascón A, Raykova M, Pinkas B. Make some ROOM for the zeros: Data sparsity in secure distributed ma-

chine learning. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. London, UK: Association for Computing Machinery, 2019. 1335−1350

114 Chaudhari H, Rachuri R, Suresh A. Trident: Efficient 4PC framework for privacy preserving machine learning. arXiv preprint arXiv: 1912.02631v2, 2021.

115 Byali M, Chaudhari H, Patra A, Suresh A. FLASH: Fast and robust framework for privacy-preserving machine learning. *Proceedings on Privacy Enhancing Technologies*, 2020, **2020**(2): 459−480

116 Tan S J, Knott B, Tian Y, Wu D J. CryptGPU: Fast privacy-preserving machine learning on the GPU. In: Proceedings of the IEEE Symposium on Security and Privacy. San Francisco, USA: IEEE, 2021. 1021−1038

117 Koti N, Pancholi M, Patra A, Suresh A. SWIFT: Super-fast and robust privacy-preserving machine learning. In: Proceedings of the 30th USENIX Security Symposium. Virtual Event: USENIX Association, 2021. 2651−2668

118 Wagh S, Tople S, Benhamouda F, Kushilevitz E, Mittal P, Rabin T. FALCON: Honest-majority maliciously secure framework for private deep learning. *Proceedings on Privacy Enhancing Technologies*, 2021, **2021**(1): 188−208

119 Fereidooni H, Marchal S, Miettinen M, Mirhoseini A, Möllering H, Nguyen T D, et al. SAFELearn: Secure aggregation for private federated learning. In: Proceedings of the IEEE Security and Privacy Workshops (SPW). San Francisco, USA: IEEE, 2021. 56−62

120 Brunetta C, Tsaloli G, Liang B, Banegas G, Mitrokotsa A. Non-interactive, secure verifiable aggregation for decentralized, privacy-preserving learning. In: Proceedings of the 26th Australasian Conference on Information Security and Privacy. Virtual Event: Springer, 2021. 510−528

121 Zheng W T, Deng R, Chen W K, Popa R A, Panda A, Stoica I. Cerebro: A platform for multi-party cryptographic collaborative learning. In: Proceedings of the 30th USENIX Security Symposium. Virtual Event: USENIX Association, 2021. 2723−2740

122 Cho H, Wu D J, Berger B. Secure genome-wide association analysis using multiparty computation. *Nature Biotechnology*, 2018, **36**(6): 547−551

123 Liu M L, Xiao L L, Zhang Z F. Multiplicative linear secret sharing schemes based on connectivity of graphs. *IEEE Transactions on Information Theory*, 2007, **53**(11): 3973−3978

124 Zhang Zhi-Fang. Secret Sharing and Multi-party Computation [Ph.D. dissertation], University of Chinese Academy of Sciences, China, 2007.
(张志芳. 密钥共享与安全多方计算 [博士学位论文], 中国科学院大学, 中国, 2007.)

125 Darup M S. Encrypted polynomial control based on tailored two-party computation. *International Journal of Robust and Nonlinear Control*, 2020, **30**(11): 4168−4187

126 Alexandru A B, Pappas G J. Secure multi-party computation for cloud-based control. *Privacy in Dynamical Systems*. Singapore: Springer, 2020. 179−207

127 Gonzalez-Serrano F J, Amor-Martln A, Casamayon-Anton J. State estimation using an extended Kalman filter with privacy-protected observed inputs. In: Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS). Atlanta, USA: IEEE, 2014. 54−59

128 Katz J, Lindell Y. *Introduction to Modern Cryptography* (3rd edition). Boca Raton: CRC Press, 2020.

129 Rivest R L, Adleman L, Dertouzos M L. On data banks and privacy homomorphisms. *Foundations of Secure Computation*. New York: Academic Press, 1978. 169−179

130 Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing. Bethesda, USA: Association for Computing Machinery, 2009. 169−178

131 Paillier P. Public-key cryptosystems based on composite degree Residuosity Classes. In: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Prague, Czech Republic: Springer, 1999. 223−238

132 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 1978, **21**(2): 120−126

133 ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 1985, **31**(4): 469−472

134 Fouque P A, Pointcheval D. Threshold cryptosystems secure against chosen-ciphertext attacks. In: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security. Gold Coast, Australia: Springer, 2001. 351−368

135 Yao A C C. How to generate and exchange secrets. In: Proceedings of the 27th Annual Symposium on Foundations of Computer Science (sfcs 1986). Toronto, Canada: IEEE, 1986. 162−167

136 Goldreich O, Micali S, Wigderson A. How to play any mental game. In: Proceedings of the 19th Annual ACM Symposium on Theory of Computing. New York, USA: Association for Computing Machinery, 1987. 218−229

137 Ben-Or M, Goldwasser S, Wigderson A. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In: Proceedings of the 20th Annual ACM Symposium on Theory of Computing. Chicago, USA: Association for Computing Machinery, 1988. 1−10

138 Chaum D, Crépeau C, Damgard I. Multiparty unconditionally secure protocols. In: Proceedings of the 20th Annual ACM Symposium on Theory of Computing. Chicago, USA: Association for Computing Machinery, 1988. 11−19

139 Rabin T, Ben-Or M. Verifiable secret sharing and multiparty protocols with honest majority. In: Proceedings of the 21st Annual ACM Symposium on Theory of Computing. Seattle, USA: Association for Computing Machinery, 1989. 73−85

140 Beaver D, Micali S, Rogaway P. The round complexity of secure protocols. In: Proceedings of the 22nd Annual ACM Symposium on Theory of Computing. Baltimore, USA: Association for Computing Machinery, 1990. 503−513

141 Lindell Y. Secure multiparty computation. *Communications of the ACM*, 2020, **64**(1): 86−96

142 Huo Wei, Yu Yu, Yang Kang, Zheng Zhong-Xiang, Li Xiang-Xue, Yao Li, et al. Privacy-preserving cryptographic algorithms and protocols: A survey on designs and applications. *Scientia Sinica Informationis*, 2023, **53**(9): 1688−1733
(霍炜, 郁昱, 杨糠, 郑中翔, 李祥学, 姚立, 等. 隐私保护计算密码技术研究进展与应用. 中国科学: 信息科学, 2023, **53**(9): 1688−1733)

143 Mo Y L, Murray R M. Privacy preserving average consensus. *IEEE Transactions on Automatic Control*, 2017, **62**(2): 753−765

144 Huang M Y, Manton J H. Coordination and consensus of networked agents with noisy measurements: Stochastic algorithms and asymptotic behavior. *SIAM Journal on Control and Optimization*, 2009, **48**(1): 134−161

145 Zhang W T, Zuo Z Q, Wang Y J, Hu G Q. How much noise suffices for privacy of multiagent systems? *IEEE Transactions on Automatic Control*, 2023, **68**(10): 6051−6066

146 Dwork C, McSherry F, Nissim K, Smith A. Calibrating noise to sensitivity in private data analysis. In: Proceedings of the 3rd Theory of Cryptography Conference. New York, USA: Springer, 2006. 265−284

147 Dwork C, Roth A. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, 2014, **9**(3−4): 211−407

148 Huang Z Q, Mitra S, Vaidya N. Differentially private distributed optimization. In: Proceedings of the 16th International Conference on Distributed Computing and Networking. Goa, India: Association for Computing Machinery, 2015. Article No. 4

149 Huang Z Q, Mitra S, Dullerud G. Differentially private iterative synchronous consensus. In: Proceedings of the ACM Workshop on Privacy in the Electronic Society. Raleigh North, USA: Association for Computing Machinery, 2012. 81–90

150 Wang Y, Huang Z Q, Mitra S, Dullerud G E. Differential privacy in linear distributed control systems: Entropy minimizing mechanisms and performance tradeoffs. *IEEE Transactions on Control of Network Systems*, 2017, **4**(1): 118–130

151 Koufogiannis F, Pappas G J. Diffusing private data over networks. *IEEE Transactions on Control of Network Systems*, 2018, **5**(3): 1027–1037

152 Le Ny J, Mohammady M. Differentially private MIMO filtering for event streams. *IEEE Transactions on Automatic Control*, 2018, **63**(1): 145–157

153 Degue K H, Le Ny J. Differentially private Kalman filtering with signal aggregation. *IEEE Transactions on Automatic Control*, 2023, **68**(10): 6240–6246

154 Le Ny J. Differentially private nonlinear observer design using contraction analysis. *International Journal of Robust and Nonlinear Control*, 2020, **30**(11): 4225–4243

155 Degue K H, Le Ny J. Differentially private interval observer design with bounded input perturbation. In: Proceedings of the American Control Conference (ACC). Denver, USA: IEEE, 2020. 1465–1470

156 Degue K H, Le Ny J. Cooperative differentially private LQG control with measurement aggregation. *IEEE Control Systems Letters*, 2023, **7**: 1093–1098

157 Nozari E, Tallapragada P, Cortés J. Differentially private distributed convex optimization via functional perturbation. *IEEE Transactions on Control of Network Systems*, 2018, **5**(1): 395–408

158 Nozari E, Tallapragada P, Cortés J. Differentially private average consensus: Obstructions, trade-offs, and optimal algorithm design. *Automatica*, 2017, **81**: 221–231

159 Liang L M, Ding R Q, Liu S, Su R. Event-triggered privacy-preserving consensus control with edge-based additive noise. *IEEE Transactions on Automatic Control*, 2024, **69**(10): 7059–7066

160 Wang L, Liu W J, Guo F H, Qiao Z X, Wu Z G. Differentially private average consensus with improved accuracy-privacy trade-off. *Automatica*, 2024, **167**: Article No. 111769

161 Liu X K, Zhang J F, Wang J M. Differentially private consensus algorithm for continuous-time heterogeneous multi-agent systems. *Automatica*, 2020, **122**: Article No. 109283

162 Wang J M, Tan J W, Zhang J F. Differentially private distributed parameter estimation. *Journal of Systems Science and Complexity*, 2023, **36**(1): 187–204

163 Wang J M, Zhang J F, Liu X K. Differentially private resilient distributed cooperative online estimation over digraphs. *International Journal of Robust and Nonlinear Control*, 2022, **32**(15): 8670–8688

164 Wang J M, Zhang J F, He X K. Differentially private distributed algorithms for stochastic aggregative games. *Automatica*, 2022, **142**: Article No. 110440

165 Chen J L, Wang J M, Zhang J F. Differentially private distributed nonconvex stochastic optimization with quantized communication. *IEEE Transactions on Automatic Control*, DOI: 10.1109/TAC.2025.3590872

166 Chen J L, Wang J M, Zhang J F. Differentially private gradient-tracking-based distributed stochastic optimization over directed graphs. arXiv preprint arXiv: 2501.06793v2, 2025.

167 Xuan Y, Wang Y Q. Gradient-tracking based differentially private distributed optimization with enhanced optimization accuracy. *Automatica*, 2023, **155**: Article No. 111150

168 Wang Y Q, Başar T. Decentralized nonconvex optimization with guaranteed privacy and accuracy. *Automatica*, 2023, **150**: Article No. 110858

169 Wang Y Q, Nedić A. Tailoring gradient methods for differentially private distributed optimization. *IEEE Transactions on Automatic Control*, 2024, **69**(2): 872–887

170 Liu C X, Johansson K H, Shi Y. Private stochastic dual averaging for decentralized empirical risk minimization. *IFAC-PapersOnLine*, 2022, **55**(13): 43–48

171 Ding T, Zhu S Y, He J P, Chen C L, Guan X P. Differentially private distributed optimization via state and direction perturbation in multiagent systems. *IEEE Transactions on Automatic Control*, 2022, **67**(2): 722–737

172 Chen F, Chen X Z, Xiang L Y, Ren W. Distributed economic dispatch via a predictive scheme: Heterogeneous delays and privacy preservation. *Automatica*, 2021, **123**: Article No. 109356

173 Hale M T, Egerstedt M. Cloud-enabled differentially private multiagent optimization with constraints. *IEEE Transactions on Control of Network Systems*, 2018, **5**(4): 1693–1706

174 Gao L, Deng S J, Ren W. Differentially private consensus with an event-triggered mechanism. *IEEE Transactions on Control of Network Systems*, 2019, **6**(1): 60–71

175 Gao L, Deng S J, Ren W, Hu C Q. Differentially private consensus with quantized communication. *IEEE Transactions on Cybernetics*, 2021, **51**(8): 4075–4088

176 Chen W, Wang Z D, Hu J, Liu G P. Differentially private average consensus with logarithmic dynamic encoding-decoding scheme. *IEEE Transactions on Cybernetics*, 2023, **53**(10): 6725–6736

177 He J P, Cai L, Guan X P. Differential private noise adding mechanism and its application on consensus algorithm. *IEEE Transactions on Signal Processing*, 2020, **68**: 4069–4082

178 Fiore D, Russo G. Resilient consensus for multi-agent systems subject to differential privacy requirements. *Automatica*, 2019, **106**: 18–26

179 Kawano Y, Cao M. Design of privacy-preserving dynamic controllers. *IEEE Transactions on Automatic Control*, 2020, **65**(9): 3863–3878

180 Kawano Y, Kashima K, Cao M. Modular control under privacy protection: Fundamental trade-offs. *Automatica*, 2021, **127**: Article No. 109518

181 Ito K, Kawano Y, Kashima K. Privacy protection with heavy-tailed noise for linear dynamical systems. *Automatica*, 2021, **131**: Article No. 109732

182 Liu L, Kawano Y, Cao M. Privacy analysis for quantized networked control systems. In: Proceedings of the 62nd IEEE Conference on Decision and Control (CDC). Singapore: IEEE, 2023. 5073–5078

183 Sugiura G, Ito K, Kashima K. Bayesian differential privacy for linear dynamical systems. *IEEE Control Systems Letters*, 2022, **6**: 896–901

184 Katewa V, Chakrabortty A, Gupta V. Differential privacy for network identification. *IEEE Transactions on Control of Network Systems*, 2020, **7**(1): 266–277

185 Han Y H, Martínez S. A numerical verification framework for differential privacy in estimation. *IEEE Control Systems Letters*, 2022, **6**: 1712–1717

186 Yan X H, Chen B, Zhang Y C, Yu L. Guaranteeing differential privacy in distributed fusion estimation. *IEEE Transactions on Aerospace and Electronic Systems*, 2023, **59**(3): 3416–3423

187 Ye M J, Hu G Q, Xie L H, Xu S Y. Differentially private distributed Nash equilibrium seeking for aggregative games. *IEEE*

Transactions on Automatic Control, 2022, **67**(5): 2451−2458

188 Sandberg H, Dán G, Thobaben R. Differentially private state estimation in distribution networks with smart meters. In: Proceedings of the 54th IEEE Conference on Decision and Control (CDC). Osaka, Japan: IEEE, 2015. 4492−4498

189 Yan X H, Chen B, Zhang Y C, Yu L. Distributed encryption fusion estimation against full eavesdropping. *Automatica*, 2023, **153**: Article No. 111025

190 Yazdani K, Jones A, Leahy K, Hale M. Differentially private LQ control. *IEEE Transactions on Automatic Control*, 2023, **68**(2): 1061−1068

191 Rizk E, Vlaski S, Sayed A H. Enforcing privacy in distributed learning with performance guarantees. *IEEE Transactions on Signal Processing*, 2023, **71**: 3385−3398

192 Rizk E, Sayed A H. A graph federated architecture with privacy preserving learning. In: Proceedings of the 22nd IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC). Lucca, Italy: IEEE, 2021. 131−135

193 Lang N, Sofer E, Shaked T, Shlezinger N. Joint privacy enhancement and quantization in federated learning. *IEEE Transactions on Signal Processing*, 2023, **71**: 295−310

194 Rostampour V, Ferrari R M G, Teixeira A M H, Keviczky T. Privatized distributed anomaly detection for large-scale nonlinear uncertain systems. *IEEE Transactions on Automatic Control*, 2021, **66**(11): 5299−5313

195 Qin S Y, He J P, Fang C R, Lam J. Differential private discrete noise-adding mechanism: Conditions, properties, and optimization. *IEEE Transactions on Signal Processing*, 2023, **71**: 3534−3547

196 Li T, Fu M Y, Xie L H, Zhang J F. Distributed consensus with limited communication data rate. *IEEE Transactions on Automatic Control*, 2011, **56**(2): 279−292

197 Dimarogonas D V, Johansson K H. Event-triggered control for multi-agent systems. In: Proceedings of the 48th IEEE Conference on Decision and Control (CDC) Held Jointly With the 28th Chinese Control Conference. Shanghai, China: IEEE, 2009. 7131−7136

198 Lv X, Hou X Y, Ren C S, Ge X, Yang P L, Cui Q M, et al. Secure and efficient federated learning with provable performance guarantees via stochastic quantization. *IEEE Transactions on Information Forensics and Security*, 2024, **19**: 4070−4085

199 The Project Team of Some Bottleneck Problems in Control Theory. *Some Bottleneck Problems in Control Theory*. Beijing: Science Press, 2022.
(控制理论若干瓶颈问题项目组. 控制理论若干瓶颈问题. 北京: 科学出版社, 2022.)

200 Söderström T. Errors-in-variables methods in system identification. *Automatica*, 2007, **43**(6): 939−958

201 Zhou K M, Doyle J C, Glover K. *Robust and Optimal Control*. Upper Saddle River: Prentice Hall, 1996.

202 Khalil H K. *Nonlinear Systems* (3rd edition). Upper Saddle River: Prentice Hall, 2001.

203 Krstic M, Kanellakopoulos L, Kokotovic P V. *Nonlinear and Adaptive Control Design*. New York: John Wiley & Sons, Inc., 1995.

204 Gorbunov S, Vaikuntanathan V, Wichs D. Leveled fully homomorphic signatures from standard lattices. In: Proceedings of the 47th Annual ACM Symposium on Theory of Computing. Portland, USA: Association for Computing Machinery, 2015. 469−477

205 Gennaro R, Wichs D. Fully homomorphic message authenticators. In: Proceedings of the 19th International Conference on Theory and Application of Cryptology and Information Security. Bengaluru, India: Springer, 2013. 301−320

206 Sun X Q, Yu F R, Zhang P, Sun Z W, Xie W X, Peng X. A survey on zero-knowledge proof in blockchain. *IEEE Network*, 2021, **35**(4): 198−205

207 Parno B, Howell J, Gentry C, Raykova M. Pinocchio: Nearly practical verifiable computation. *Communications of the ACM*, 2016, **59**(2): 103−112

208 Chida K, Hamada K, Ikarashi D, Kikuchi R, Genkin D, Lindell Y, et al. Fast large-scale honest-majority MPC for malicious adversaries. *Journal of Cryptology*, 2023, **36**(3): Article No. 15

209 Keller M, Orsini E, Scholl P. MASCOT: Faster malicious arithmetic secure computation with oblivious transfer. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria: Association for Computing Machinery, 2016. 830−842

210 Regev O. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 2009, **56**(6): Article No. 34

211 Abdalla M, Bourse F, de Caro A, Pointcheval D. Simple functional encryption schemes for inner products. In: Proceedings of the 18th IACR International Conference on Practice and Theory in Public-key Cryptography. Gaithersburg, USA: Springer, 2015. 733−751

212 Agrawal S, Libert B, Stehlé D. Fully secure functional encryption for inner products, from standard assumptions. In: Proceedings of the 36th Annual International Cryptology Conference. Santa Barbara, USA: Springer, 2016. 333−362

213 Weng C H, Nekouei E, Johansson K H. Optimal privacy-aware dynamic estimation. arXiv preprint arXiv: 2311.05896, 2023.

214 Wang L, Cao X H, Zhang H, Sun C Y, Zheng W X. Transmission scheduling for privacy-optimal encryption against eavesdropping attacks on remote state estimation. *Automatica*, 2022, **137**: Article No. 110145

215 Shu H Y, Zhou J Y, Yang W, Zhang H. Distortion-based state security codes for distributed sensor networks. *Automatica*, 2023, **151**: Article No. 110904

216 Umsonst D, Sandberg H. On the confidentiality of controller states under sensor attacks. *Automatica*, 2021, **123**: Article No. 109329

217 Katewa V, Anguluri R, Pasqualetti F. On a security vs privacy trade-off in interconnected dynamical systems. *Automatica*, 2021, **125**: Article No. 109426

218 Wang H J, Liu K, Li B J, Fridman E, Xia Y Q. Privacy and security trade-off in interconnected systems with known or unknown privacy noise covariance. *Automatica*, 2025, **173**: Article No. 112071

219 Wonham W M. *Linear Multivariable Control: A Geometric Approach* (3rd edition). New York: Springer, 1985.

220 Huang Y H, Huang L N, Zhu Q Y. Reinforcement Learning for feedback-enabled cyber resilience. *Annual Reviews in Control*, 2022, **53**: 273−295

221 Zhang K K, Keliris C, Polycarpou M M, Parisini T. Detecting stealthy integrity attacks in a class of nonlinear cyber-physical systems: A backward-in-time approach. *Automatica*, 2022, **141**: Article No. 110262

222 Jiang P P, Wang Q, Huang M Q, Wang C, Li Q, Shen C, et al. Building in-the-cloud network functions: Security and privacy challenges. *Proceedings of the IEEE*, 2021, **109**(12): 1888−1919

223 Bharathi B, Manivasagam G, Kumar M A. Metrics for performance evaluation of encryption algorithms. *International Journal of Advance Research in Science and Engineering*, 2017, **6**(3): 62−72

224 Wang C, Ren K, Wang J. Secure optimization computation outsourcing in cloud computing: A case study of linear programming. *IEEE Transactions on Computers*, 2016, **65**(1): 216−229

225 Khan M A, Puri D. Challenges and opportunities in implementing quantum-safe key distribution in IoT devices. In: Pro-

ceedings of the 3rd International Conference for Innovation in Technology (INOCON). Bangalore, India: IEEE, 2024. 1−7

226 Jacob R, Lesage J J, Faure J M. Overview of discrete event systems opacity: Models, validation, and quantification. *Annual Reviews in Control*, 2016, **41**: 135−146

227 John V M, Katewa V. Opacity versus security in linear dynamical systems. *IEEE Transactions on Automatic Control*, 2025, **70**(1): 323−338

228 Liu R J, Lu J Q. Enforcement for infinite-step opacity and K-step opacity via insertion mechanism. *Automatica*, 2022, **140**: Article No. 110212

229 Yin X, Li Z J, Wang W L, Li S Y. Infinite-step opacity and *K*-step opacity of stochastic discrete-event systems. *Automatica*, 2019, **99**: 266−274

230 Hou J Y, Yin X, Li S Y. A framework for current-state opacity under dynamic information release mechanism. *Automatica*, 2022, **140**: Article No. 110238

231 Tong Y, Lan H, Seatzu C. Verification of *K*-step and infinite-step opacity of bounded labeled Petri nets. *Automatica*, 2022, **140**: Article No. 110221

232 An L W, Yang G H. Opacity enforcement for confidential robust control in linear cyber-physical systems. *IEEE Transactions on Automatic Control*, 2020, **65**(3): 1234−1241

233 Xie Y F, Li S Y, Yin X. Optimal synthesis of opacity-enforcing supervisors for qualitative and quantitative specifications. *IEEE Transactions on Automatic Control*, 2024, **69**(8): 4958−4973

234 Ramasubramanian B, Cleaveland R, Marcus S I. Notions of centralized and decentralized opacity in linear systems. *IEEE Transactions on Automatic Control*, 2020, **65**(4): 1442−1455

235 Lu Y, Zhu M H. On privacy preserving data release of linear dynamic networks. *Automatica*, 2020, **115**: Article No. 108839

236 Ji Y D, Yin X, Lafortune S. Opacity enforcement using nondeterministic publicly known edit functions. *IEEE Transactions on Automatic Control*, 2019, **64**(10): 4369−4376

237 Liu R J, Lu J Q, Hadjicostis C N. Opacity enforcement via attribute-based edit functions in the presence of an intended receiver. *IEEE Transactions on Automatic Control*, 2023, **68**(9): 5646−5652

238 Li X Y, Hadjicostis C N, Li Z W. Extended insertion functions for opacity enforcement in discrete-event systems. *IEEE Transactions on Automatic Control*, 2022, **67**(10): 5289−5303

239 Keroglou C, Lafortune S. Embedded insertion functions for opacity enforcement. *IEEE Transactions on Automatic Control*, 2021, **66**(9): 4184−4191

240 Ji Y D, Wu Y C, Lafortune S. Enforcement of opacity by public and private insertion functions. *Automatica*, 2018, **93**: 369−378

241 Xie Y F, Yin X, Li S Y. Opacity enforcing supervisory control using nondeterministic supervisors. *IEEE Transactions on Automatic Control*, 2022, **67**(12): 6567−6582

242 Chen W, Wang Z D, Liu Q Y, Yue D, Liu G P. A new privacy-preserving average consensus algorithm with twophase structure: Applications to load sharing of microgrids. *Automatica*, 2024, **167**: Article No. 111715

243 Zhang K X, Li Z J, Wang Y Q, Louati A, Chen J. Privacy-preserving dynamic average consensus via state decomposition: Case study on multi-robot formation control. *Automatica*, 2022, **139**: Article No. 110182

244 Spiekermann S, Korunovska J, Langheinrich M. Inside the organization: Why privacy and security engineering is a challenge for engineers. *Proceedings of the IEEE*, 2019, **107**(3): 600−615

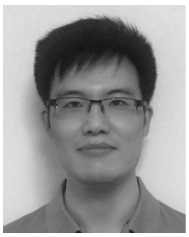
245 Hu C Q, Zhuang H J, Chen J J, Hu P F, Xiang T, Yu J G. Achieving privacy-preserving online multi-layer perceptron model in smart grid. *IEEE Transactions on Cloud Computing*, 2024, **12**(2): 777−788

246 Donnelly W, Keifer P, Minor R, Muthukumaran U, Parolek B, Tuck B, et al. A review of privacy-preserving and efficient data collection and aggregation in smart grids. In: Proceedings of the 11th International Conference on Information and Communication Technology (ICoICT). Melaka, Malaysia: IEEE, 2023. 326−332

247 Gao H, Li Z J, Wang Y Q. Privacy-preserving collaborative estimation for networked vehicles with application to collaborative road profile estimation. *IEEE Transactions on Intelligent Transportation Systems*, 2022, **23**(10): 17301−17311

248 Das D, Banerjee S, Chatterjee P, Ghosh U, Biswas U. Blockchain for intelligent transportation systems: Applications, challenges, and opportunities. *IEEE Internet of Things Journal*, 2023, **10**(21): 18961−18970

249 Bost R, Fouque P A. Security-efficiency tradeoffs in searchable encryption. *Proceedings on Privacy Enhancing Technologies*, 2019, **2019**(4): 132−151



王继民 北京科技大学自动化学院副教授. 主要研究方向为隐私保护, 系统辨识和网络化控制系统.
E-mail: jimwang@ustb.edu.cn
(**WANG Ji-Min** Associate professor at the School of Automation and Electrical Engineering, University of Science and Technology Beijing. His research interest covers privacy protection, system identification, and networked control systems.)

张纪峰 中国科学院数学与系统科学研究院研究员. 主要研究方向为隐私保护, 系统建模与辨识, 随机系统, 适应控制, 多个体系统和有限信息系统. 本文通信作者.
E-mail: jif@iss.ac.cn
(**ZHANG Ji-Feng** Researcher at the Academy of Mathematics and Systems Science, Chinese Academy of Sciences. His research interest covers privacy protection, system modeling and identification, stochastic systems, adaptive control, multi-agent systems, and finite-bite information systems. Corresponding author of this paper.)

陈嘉龙 中国科学院数学与系统科学研究院博士研究生. 主要研究方向为隐私保护, 分布式优化和随机系统.
E-mail: chenjialong@amss.ac.cn
(**CHEN Jia-Long** Ph.D. candidate at the Academy of Mathematics and Systems Science, Chinese Academy of Sciences. His research interest covers privacy protection, distributed optimization, and stochastic systems.)