附件1-2

《隐私计算密码融合机制技术指南》团体标准编制说明

一、工作简况

（一）任务来源

2024年新发布的《网络数据安全管理条例》第十条中明确指出“网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求，在网络安全等级保护的基础上，加强网络数据安全防护，建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用，处置网络数据安全事件，防范针对和利用网络数据实施的违法犯罪活动，并对所处理网络数据的安全承担主体责任。”为了进一步推动数据安全技术在国内的发展，保障公民和国家隐私数据的安全，发挥北京理工大学在数据安全技术发展中的协调作用，北京理工大学联合济南超级计算技术研究院、重庆市科学技术研究院，在2025年启动了团体标准制订计划，以标准化的形式主动服务社会，引导行业健康可持续发展，建立统一市场体系、保障市场公平。

（二）主要工作过程

2025年2月—3月，北京理工大学组织召开了标准化工作启动会，明确了《隐私计算密码融合机制技术指南》标准化对象与标准化需求，成立团体标准编制小组，小组成员对隐私计算系统

的安全增强手段进行调研分析，参考相关标准和规范文件，起草了标准草案。

2025 年 4 月，北京理工大学牵头，邀请济南超级计算技术研究院、重庆市科学技术研究院对标准进行讨论，修改完善形成征求意见稿。

2025 年 5 月—7 月，标准编制小组对标准初稿进行了进一步的修改完善，并提交山东科技咨询协会（以下简称协会）。

2025 年 11 月 6 日，协会标准化建设专业委员会组织召开团体标准立项评审会。会议邀请山东师范大学、山东省计算中心（国家超级计算济南中心）等单位的 3 位专家，对北京理工大学起草的《联邦学习场景的安全可信技术指南》《隐私计算密码融合机制技术指南》两项团体标准进行立项评审。会上，评审专家听取了标准起草组对两项团体标准立项的目的意义、适用范围、主要技术内容等方面的汇报，审阅了立项申请材料，逐项对标准草案及编制说明内容进行质询和研讨，并出具了立项评审意见。评审专家一致认为《联邦学习场景的安全可信技术指南》《隐私计算密码融合机制技术指南》两项团体标准符合立项条件，同意立项。

二、标准编制原则、主要内容及其确定依据

（一）标准编制原则

本标准的编制，严格遵循统一性、协调性、适用性、一致性、规范性五大原则，依据 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》进行起草。旨在保证标准

具有规范性；规定明确且无歧义的条款；清楚和准确；能被未参加标准编制的专业人员所理解；标准内容便于实施。

（二）主要内容

本标准主要包括范围、规范性引用文件、术语和定义、系统架构与关键要素、技术分类与融合路径、应用场景与解决方案等内容。

（1）范围:

本文件旨在提供隐私计算技术在分布式计算场景下的实施框架、关键技术与应用指南，适用于在数据不出域的前提下，通过联邦学习和密码融合技术，实现联合建模与协同计算的应用需求。

（2）术语和定义:

本文件定义了多方安全计算、联邦学习、参与方、安全模型等与隐私计算密码融合机制相关的核心概念和专业术语。

（3）概述:

本文件阐述了隐私计算中密码融合机制的基本概念，即通过多种密码学方法协同实现数据保护与安全计算，并提出了机密性、完整性、可验证性等基本安全要求。

（4）系统架构与关键要素:

本文件详细描述了隐私计算系统的组成，包括本地计算节点、协同调度中心、安全计算模块等，并明确了数据提供方、模型协调方等参与方角色，以及从任务配置到结果输出的密码融合

流程和关键安全要素。

（5）技术分类与融合路径:

本文件梳理了隐私计算中常用的密码学技术类型（如MPC、HE、TEE、DP），适配的协同计算模式，并分析了串联式、并行式和桥接式等多种融合策略与组合方式。

（6）应用场景与解决方案:

本文件将密码融合机制应用于数据统计、数据匹配和联合建模等典型多方协同场景，并针对不同场景提供了详细的技术选型建议，以指导实际系统设计与部署。

（7）隐私保护效果评估与验证:

本文件从总体要求、评价维度与指标、评估方法及验证报告等方面，对采用密码融合机制的隐私计算系统提出了可执行的隐私保护效果评估与验证框架，为方案选型与优化提供量化依据，并为系统验收、风险管理和监管审查提供可审计、可复用的支撑。

（三）确定主要内容的依据

本团体标准主要内容的确定，是基于对国家战略需求、行业发展趋势，以及技术演进特点的综合考量。

本标准严格遵循国家在网络安全、数据安全和个人信息保护方面的法律法规及政策导向，如《中华人民共和国网络安全法》《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》等。特别是响应了“数据二十条”中提出的“原始数据不出域、数据可用不可见”原则，旨在为数据要素的安全流通与价

值释放提供关键技术支撑。

鉴于当前各行各业对安全多方数据协同计算的迫切需求，以及现有标准体系在隐私计算、特别是密码融合机制领域尚存空白，本标准旨在填补这一不足。本标准致力于解决数据孤岛、数据滥用和隐私泄露等现实痛点，为各安全敏感型领域提供安全可信的数据协同解决方案。

此外，本标准内容是基于对同态加密、多方安全计算、可信执行环境等前沿密码学技术及其融合应用趋势的深入研究与实践总结。通过明确系统架构、技术分类、融合策略及应用场景，本标准旨在规范隐私计算密码融合机制的研发与应用，提升系统的安全性、可靠性与互操作性，从而有力促进数据要素市场的健康发展。

三、试验（或验证）的分析报告、技术经济论证以及预期效益

本标准在编制过程中，结合典型分布式计算与隐私计算系统，对多种密码协议组合进行了原型实现与对比试验。在遵循现行信息安全、联邦学习和隐私计算等相关标准的基础上，重点考察了多协议协同、密钥管理和审计验证等环节的效果。试验结果表明，本标准提出的密码融合架构和协议组合策略，在满足通用安全要求的同时，可降低中间信息暴露风险，增强协同计算过程的可验证性和稳健性。

从技术经济角度看，隐私计算密码融合机制已具备工程应用

的基本可行性，能够支撑“数据不出域”条件下的数据统计、数据匹配和联合建模需求。现行相关标准对密码融合架构、跨协议数据转换和密钥全生命周期协同管理缺乏统一规范，实践中往往依赖大量定制化设计与反复验证，增加了建设成本和试错成本。本标准通过给出典型融合路径、角色划分和评估要点，为系统集成提供了可复用的设计参考，有助于压缩方案收敛时间和实施成本。

在预期效益方面，本标准的实施有望弥补现有标准体系在隐私计算密码融合机制方面的细化不足，推动隐私计算技术在金融、医疗、政务等行业的规范落地，提升个人信息和敏感数据保护水平，促进数据要素在可控条件下安全流通，为数字经济发展和相关产业生态完善提供支撑。

四、与现行相关法律、法规及相关标准的关系

本标准与现行法律、法规统一，协调一致，并与现行有效的国家标准和行业标准有很好的协调性，形成协同效应，共同构建完善的数据安全和隐私保护标准体系。

五、采用国际标准和国外先进标准情况，与国际、国外同类标准水平的对比情况，国内外关键指标对比分析或与测试的国外样品、样机的相关数据对比情况

本标准在编制过程中参考或引用相关标准

GB/T 25069-2022 信息安全技术术语

YD/T 4691-2024 隐私计算联邦学习产品安全要求和测试方

法

YD/T 4581-2023 隐私保护场景下安全多方计算技术指南

YD/T AAAA-AAAA 术语和定义

T/CCSA 407-2022 术语和定义

六、标准中如果涉及专利，应有明确的知识产权说明

本标准中不涉及专利。

七、重大分歧意见的处理过程、处理意见及其依据

本标准的制定过程中未出现重大的分歧意见。

八、实施标准的要求以及相关措施建议

为了使标准得到更好更有效的实施，应组织相关管理人员、技术人员和操作人员进行标准宣贯培训，使所有的技术人员和操作人员都能灵活掌握本标准的详细条款和具体要求，并在实际工作中得到认真的贯彻和执行。

标准编写组后续也将及时收集各单位在标准实施中的意见及建议，并在适当的时候对标准进行修订。

九、其他应当说明的事项

无。

《隐私计算密码融合机制技术指南》团体标准

标准起草组

2025 年 12 月