ICS 35.240
CCS L 67

中华人民共和国国家标准化指导性技术文件

GB/Z 191—2026

智能计算　隐私保护计算技术框架

Intelligent computing—Technical framework of privacy-preserving computation

2026-07-02 发布

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件为规范类指导性技术文件。

本文件按照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》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国智能计算标准化工作组(SAC/SWG 32)提出并归口。

本文件起草单位：蚂蚁科技集团股份有限公司、浙江大学、中国电信集团有限公司、之江实验室、中国移动通信集团有限公司、浪潮电子信息产业股份有限公司、北京数字认证股份有限公司、中国联合网络通信有限公司软件研究院、杭州趣链科技有限公司、洞见科技(雄安)有限公司、浙江大数据交易中心有限公司、华控清交信息科技(北京)有限公司、杭州锘崴信息科技有限公司、联通数据智能有限公司、北京国际大数据交易所有限责任公司、浙江蚂蚁密算科技有限公司、京东科技信息技术有限公司、浪潮云信息技术股份公司、杭州安恒信息技术股份有限公司、蚂蚁区块链科技(上海)有限公司、中国汽车工程研究院股份有限公司、海光信息技术股份有限公司、马上消费金融股份有限公司、湖北华中电力科技开发有限责任公司、华为技术有限公司、中国计量大学、北京华成智云软件股份有限公司、北京数安行科技有限公司、联通(海南)产业互联网有限公司、北京联想软件有限公司、深圳陆兮科技有限公司。

本文件主要起草人：韦韬、任奎、昌文婷、杨坤、崔娜妮、张永强、杨白雪、彭晋、茹志强、李博、李振廷、李帜、谢志勇、肖雪、贾晓芸、李国庆、贺皓、潘禹霖、孔俊、袁鹏程、靳晨、张晓蒙、潘无穷、张秉晟、盛晶、聂桂兵、娄健、刘焱、王兵、周李京、陈怡晨、陈晓丰、王云浩、杨朋霖、陈钰炜、李冠洲、冯新宇、郑佳佳、韩冬、谭伊舒、孙琪、刘玉红、周芃、张世富、张汉宁。

智能计算　隐私保护计算技术框架

1　范围

本文件规定了隐私保护计算的基本要求、参考架构、协作机制、技术和安全要求。

本文件适用于隐私保护计算的规划、开发、评估和应用。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 46572—2025　智能计算　术语

3　术语和定义

GB/T 46572—2025 界定的以及下列术语和定义适用于本文件。

3.1

隐私保护计算　privacy-preserving computation

在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一类信息技术，保障数据在产生、存储、计算、应用、销毁等环节中的安全性和可用性。

注 1：隐私保护计算的常用技术方案有安全多方计算、联邦学习、可信执行环境、密态计算等。

注 2：常用的底层技术有混淆电路、不经意传输、秘密分享、同态加密等。

3.2

原始数据　raw data

数据提供方提供的、用于输入隐私保护计算的明文数据。

[来源：GM/T 0135—2024，3.10，有修改]

3.3

敏感数据　sensitive data

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的信息或数据。

注：敏感信息数据的泄露、修改、破坏或丢失对人或事产生可预知的损害。

[来源：GB/T 35273—2020，3.2，有修改]

3.4

中间数据　intermediate data

原始数据经加密、分片等处理后的非明文形态数据。

3.5

计算结果　computation result

隐私保护计算（3.1）输出的、供结果使用方获取的结果数据。