

ICS 35.240

CCS L 80

中华人民共和国行业标准

YD/T XXXXX—XXXX

隐私保护场景下安全多方计算技术指南

Technical guidelines of secure multi-party computation for privacy preserving

报批稿

行业标准信息服务平台

XXXX - XX - XX 发布

XXXX - XX - XX 实施

中华人民共和国工业和信息化部
布

发

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 MPC 概述	2
6 MPC 体系架构	2
6.1 MPC 系统架构	2
6.2 MPC 参与者角色	3
6.3 MPC 工作流程	4
6.4 MPC 参与者类型	4
7 MPC 安全分类	4
7.1 MPC 安全分类框架	4
7.2 MPC 安全分类	5
8 基于 MPC 的隐私保护场景及解决方案	6
8.1 数据统计类	6
8.2 数据匹配类	7
8.3 联合建模类	7

行业标准信息服务平台

前 言

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的责任。

本文件由中国通信标准化协会提出并归口。

本文件起草单位：阿里巴巴（中国）有限公司、蚂蚁科技集团股份有限公司、中国信息通信研究院、国家计算机网络应急技术处理协调中心、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国电信集团有限公司、中兴通讯股份有限公司。

本文件主要起草人：白晓媛、洪澄、朱红儒、李克鹏、陈湑、闫树、舒敏、王文磊、刘利军、王志军、肖吉、林兆骥、汪来富。

行业标准信息服务平台