隐私计算联盟
Privacy Preserving Computing Alliance

隐私计算白皮书

（2022 年）

隐私计算联盟

2022 年 12 月

版权声明

编写委员会

❖ **主要编写单位**（排名不分先后）：

隐私计算联盟、京东科技信息技术股份有限公司、北京数牍科技有限公司、蚂蚁科技集团股份有限公司、蚂蚁区块链科技（上海）有限公司、上海富数科技有限公司、上海浦东发展银行股份有限公司、洞见智慧科技有限公司、同盾科技有限公司

❖ **参与编写单位**（排名不分先后）：

优刻得科技股份有限公司、阿里巴巴（中国）有限公司、北京八分量信息科技有限公司、杭州安恒信息技术股份有限公司、杭州卷积云科技有限公司、西安交通大学、杭州趣链科技有限公司、浙江吉利数字科技有限公司、杭州金智塔科技有限公司、北京百度网讯科技有限公司、京信数据科技有限公司、联通数字科技有限公司、杭州锘崴信息科技有限公司、上海零数科技有限公司、腾讯云计算（北京）有限责任公司、天冕信息技术（深圳）有限公司、深圳前海微众银行股份有限公司、 星环信息科技（上海）股份有限公司、深圳致星科技有限公司 、翼健（上海）信息科技有限公司、北京冲量在线科技有限公司、交通银行股份有限公司、中国移动通信有限公司研究院、中兴通讯股份有限公司、中国工商银行软件开发中心

❖ **编写组主要成员**（排名不分先后）：

贾　轩	闫　树	袁　博	王思源
杨靖世	王丹阳	童锦瑞	宋佳楠
魏　凯	姜春宇	白玉真	吕艾临
刘嘉夕	马智华	杨　博	孙中伟
金银玉	单进勇	李宏宇	张晓蒙
昌文婷	彭　晋	卞　阳	杨天雅
周　骏	冯云青	陶建萍	李　博
袁志烨	李绍宾	黄翠婷	陈　涛
潘　榕	刘　沛	金　朵	王铀之
何志坚	任雪斌	杨树森	徐　静
李晨龙	吴　凯	薛　勇	陈超超
周吉文	于　欢	汤克云	崔玲龙
王　帅	兰春嘉	李克鹏	吴焕明
葛　娴	唐　恺	苗天麒	马　轩
王光中	周　边	李　崇	郭海生
黄司辉			

前　言

我国高度重视数据安全流通技术的发展应用，过去一年内多个部门密集出台了一系列战略、规划和政策，强调数据要素流通的重要性，提出数据安全流通的建设方案。2022 年 1 月国务院办公厅印发的《要素市场化配置综合改革试点总体方案》中提出，探索“原始数据不出域、数据可用不可见”的交易范式。12 月 19 日，中共中央、国务院发布的《关于构建数据基础制度更好发挥数据要素作用的意见》提出要建立数据产权分置的产权运行机制，建立合规高效的数据要素流通和交易制度，从数据产权、流通交易、收益分配、安全治理等四项制度提出二十条政策举措，初步形成我国数据基础制度的“四梁八柱”。

隐私计算技术作为保障数据安全流通的有效方式，在政策驱动和市场需求同时作用下，乘时乘势高速发展，已逐渐成为促进数据要素跨域流通和应用的核心技术，广泛应用于金融、政务、医疗、能源、制造等诸多领域。

2021 年，中国信通院云大所联合隐私计算联盟发布《隐私计算白皮书（2021 年）》，全面展示了隐私计算发展状况。经过一年多的发展，隐私计算在政策、技术、应用等方面上均迎来了新的进展。《隐私计算白皮书（2022 年）》将全面展现行业成就及发展新态势，希望为产业界应用隐私计算技术提供参考指导，推动隐私计算行业健康发展，让隐私计算在数据要素市场建设过程中发挥更大的价值。

本研究报告亮点如下:

- 纵览发展历程，明确当前进展

根据隐私计算技术出现、发展、落地到广泛应用的不同特点，梳理隐私计算发展阶段，明确当下发展阶段并研判未来发展前景。

- 把握技术前沿，洞察发展趋势

作为数据安全流通的关键技术，隐私计算技术向推动应用落地的方向持续发展，可用性和可信性进一步增强。通过对技术发展的前沿进行整理和分析，洞察隐私计算技术发展趋势，为落地应用搭建桥梁。

- 聚焦应用实际，凸显应用优势

在广泛调研的基础上全面梳理隐私计算在实际数据流通中的最新应用情况，深度剖析隐私计算发挥巨大价值的内在逻辑，更加清晰地回答“隐私计算与传统数据流通技术相比有何优势”“哪些特定创新场景只有隐私计算能够解决”等问题，进一步明确隐私计算优势，促进隐私计算应用发展。

- 综述行业现状，梳理发展热点

通过对隐私计算商业模式、市场规模、科研、开源、互联互通等行业情况进行综述及分析，梳理隐私计算安全性、性能、互联互通、合规性等发展热点，把握行业整体脉络，为战略布局提供参考。

道阻且长，行则将至；行而不辍，未来可期。面对这个日新月异、快速发展的行业，我们期待与业界共同守正创新，推动隐私计算行业健康发展，让隐私计算在数据要素市场建设和数据流通过程中发挥更大的价值，踔厉奋发谱写隐私计算新篇章！

目 录

图 目 录

表 目 录

一、隐私计算概述

（一） 隐私计算在政策和需求驱动下快速发展

自 2019 年党的十九届四中全会首次将数据列为生产要素，高速发展的数字经济已经成为带动中国经济增长的核心动力之一。我国数字经济规模由 2017 年的 27.2 万亿元增至 2021 年的 45.5 万亿元，总量稳居世界第二，年均复合增长率达 13.6%。然而，数据要素本身往往含有敏感信息，面临着流通后的数据滥用、信息泄漏和信息可被反推等隐私安全风险，因此数据安全流通开始引发广泛关注。

在政策布局上，我国高度重视数据安全流通的发展应用，过去一年内多个部门密集出台了一系列战略、规划和政策，强调数据要素流通的重要性，提出数据安全流通的发展规划。2022 年 1 月国务院发布的《“十四五”数字经济发展规划》中提出加快构建数据要素市场规则，促进数据要素市场流通。同月，国务院办公厅印发的《要素市场化配置综合改革试点总体方案》中提出，探索“原始数据不出域、数据可用不可见”的交易范式，探索建立数据用途和用量控制制度，实现数据使用“可控可计量”。今年 4 月，《中共中央国务院关于加快建设全国统一大市场的意见》提出加快培育数据要素市场，建立健全数据安全、权利保护、跨境传输管理、交易流通、开放共享、安全认证等基础制度和标准规范，深入开展数据资源调查，推动数据资源开发利用。12 月 19 日，中共中央、国务院发布的《关于构建数据基础制度更好发挥数据要素作用的意见》提出要建立数据产权分置的产权运行机制，建立合规高效的数据要素流通和交易制度，从数据产权、

流通交易、收益分配、安全治理等四项制度提出二十条政策举措，初步形成我国数据基础制度的“四梁八柱”。

隐私计算技术作为保障数据安全流通的有效方式，乘时乘势高速发展，已逐渐成为促进数据要素跨域流通和应用的核心技术，广泛应用于金融、政务、医疗、能源、制造等诸多领域。2020 年 4 月，《工业和信息化部关于工业大数据发展的指导意见》提出，激发工业数据市场活力，支持开展数据流动关键技术攻关，建设可信的工业数据流通环境。2021 年 5 月印发的《全国一体化大数据中心协同创新体系算力枢纽实施方案》提出，促进数据有序流通，试验多方安全计算、区块链、隐私计算、数据沙箱等技术模式，构建数据可信流通环境，提高数据流通效率。2022 年 10 月国务院办公厅印发的《全国一体化政务大数据体系建设指南》提出探索利用核查、模型分析、隐私计算等多种手段，有效支撑地方数据资源深度开发利用。

对隐私计算产业来说，在政策利好的持续推动下，行业市场发展与技术不断更新，技术体系不断完善，行业标准日趋统一，应用场景逐渐丰富，隐私计算产业将持续面临着良好的发展环境。

（二）隐私计算正处于产业增长期阶段

隐私计算技术可以追溯到 1949 年由香农开启的现代密码学时代，之后其内涵、特征及代表技术不断演进，融合了密码学、人工智能、计算机科学以及安全硬件等众多领域技术。直到 2001 年，国外正式提出“隐私增强技术”（Privacy Enhancing Technologies, PETs）的概念。国内也于 2016 年的《隐私计算研究范畴及发展趋势》中正式提

出“隐私计算”一词。

根据隐私计算技术出现、发展、落地到广泛应用的不同特点，我们将隐私计算的发展历程划分为四个阶段（如图 1）：

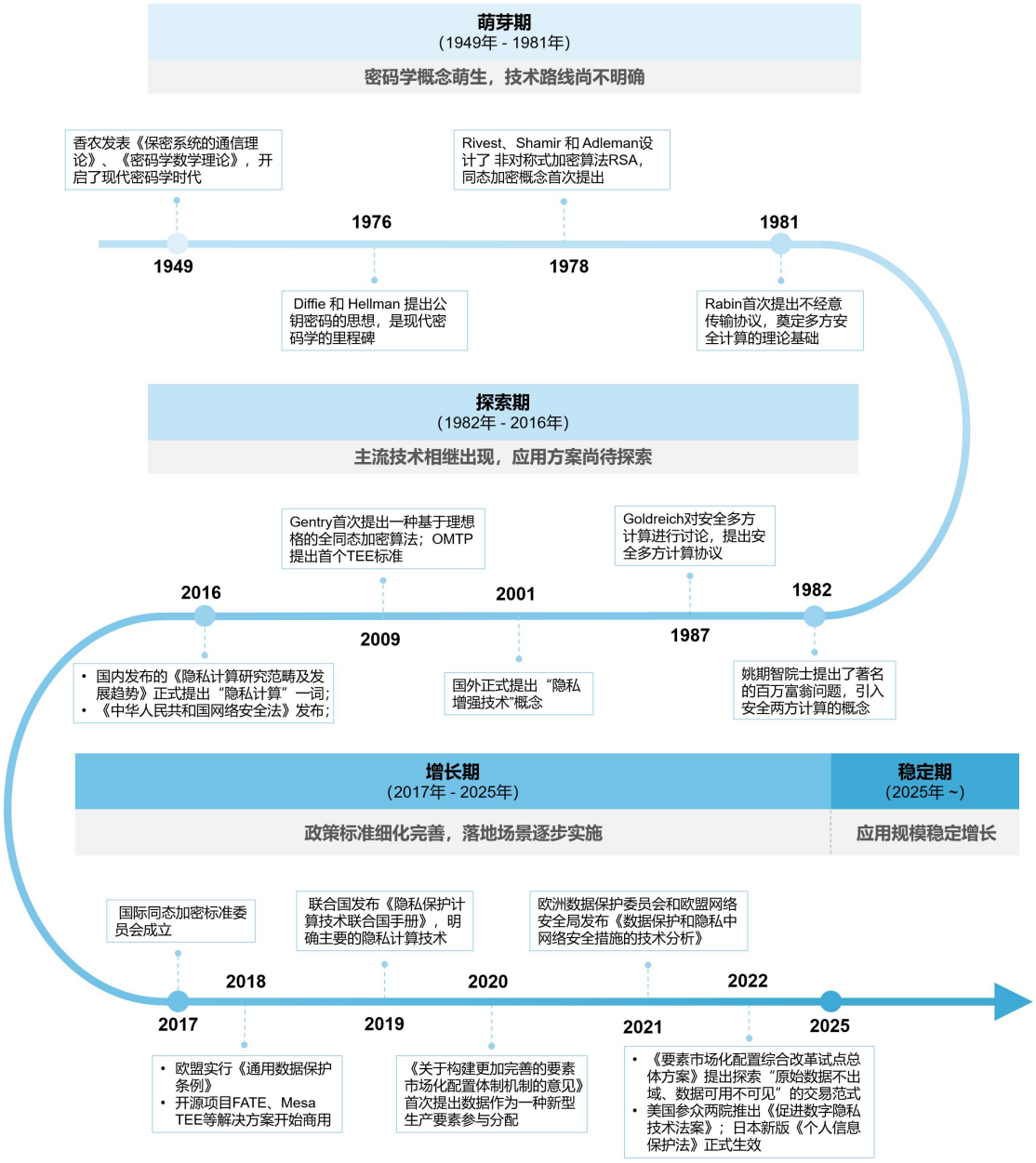

图 1 隐私计算四个发展阶段

萌芽期（1949 年-1981 年）：需求出现，概念萌芽。起始于 20 世纪 40 年代，现代信息学之父克劳德·香农的一篇重要论文《保密系统的通信理论》，被认为是现代密码学时代的开端。

探索期（1982 年-2016 年）：主流技术路线出现。随着多方安全计算、联邦学习、可信执行环境等隐私计算技术的出现和发展，隐私计算的技术栈日趋成熟。

增长期（2017 年-2025 年）：多行业的需求方和厂商陆续加入，专利、论文、标准、政策、实施案例相继涌现。该时期各国政府逐渐加强对数据安全和个人隐私保护的重视，各项政策法规陆续制定，基于隐私计算技术的数据流通产品得到不断探索应用和落地实施。

稳定期（2025 年~）：未来，随着政策和法律的清晰明确，技术进一步成熟，隐私计算作为“数据流通基础设施”将被大众广泛接受。随着“隐私计算+”发展，行业应用稳步推进，更多大型企业开始全面使用隐私计算技术，应用规模稳定增长。

当前，隐私计算仍处于产业快速增长期，即将迈入前景广阔的稳定期。随着国家数据要素市场的加速建设，隐私计算技术将在更多场景得到广泛应用，“原始数据不出域，数据可用不可见”将成为多数行业数据流通的交易范式。除了实现“数据可用不可见”外，未来还需要进一步对数据的用途和用量进行控制和审计，真正实现数据使用的“可控可计量”，最大限度的保障数据要素流动过程中数据提供方的合法权益。此外，在工业界，随着国内外政策法规的不断完善，再加上对于某些数据高敏感行业强监管的需求，数据规模不断扩大，直接在中心服务器上计算或学习的压力会不断增加，从中心化向分布式或去中心化过渡的演化也将成为未来趋势。根据《Gartner 2022 隐私技术成熟度曲线》研究报告表明：预计在未来 5~10 年内，隐私计算

技术会被大规模商业化应用。预计到 2025 年，60%以上的大型组织将在数据分析、商业智能或云计算中使用一种或多种隐私计算技术。

二、技术分析

隐私计算（Privacy-preserving computation）是指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系列信息技术，能够保障数据在流通与融合过程中的“可用不可见”。2022 年，隐私计算迎来一系列创新与突破，一方面，各主流隐私计算技术路线持续迭代优化，在单点层面提升了能力上限；另一方面，为了适应现实场景，开始探索通过技术融合等方式来突破瓶颈。技术的不断发展，使得隐私计算的可用性进一步提升，为技术大规模落地应用提供了必要条件。随着隐私计算在数据流通中的实践应用逐渐深入，行业对于隐私计算技术的安全可证、流程可控、高效稳定、开放普适等方面均提出了更高要求，隐私计算的概念得到进一步外延，逐步形成了广义隐私计算技术体系。

（一） 多方安全计算可用性进一步提升

多方安全计算（Secure Multi-party Computation，MPC）是指在无可信第三方的情况下，多个参与方共同计算一个目标函数，并且保证每一方仅获取自己的计算结果，无法通过计算过程中的交互数据推测出其他任意一方的输入数据（除非函数本身可以由自己的输入和获得的输出推测出其他参与方的输入）。该技术由图灵奖获得者姚期智院士于 1982 年通过提出和解答百万富翁问题而创立。多方安全计算是多种密码学基础工具的综合应用，除混淆电路、秘密分享、不经

意传输等密码学原理构造的经典多方安全计算协议外，其它所有用于实现多方安全计算的密码学算法都可以构成多方安全计算协议，因此在实现多方安全计算时也应用了同态加密、零知识证明等密码学算法。

多方安全计算能够在不泄漏任何隐私数据的情况下，使多个非互信主体在数据相互保密的前提下进行高效数据融合计算，并获得准确结果，达到“数据可用不可见”。最终实现数据的持有权和数据使用权相互分离，并控制数据的用途和用量，即某种程度上的“用途可控可计量”。多方安全计算具有很高的安全性，要求敏感的中间计算结果也不可以泄漏，并且在近 40 年的发展中其各种核心技术和构造方案不断接受学术界和工业界的检验，具有很高的可信性，其性能在各种研究中不断提升，在很多场景下已经达到了产业能实际应用接受的程度。

2022 年，针对多方安全计算的研究与创新主要集中在性能优化和应用扩展两大方向。

在性能优化方面，使用多方安全计算技术通常会带来高额的通信和计算成本，如何在固定的安全模型下，满足现实可用的性能要求，成为了业内探索的一大关键问题。解决该问题的一种方式是通过优化算法协议，降低整个计算过程的计算复杂度和通信复杂度。例如，USENIX Security’22 上发布的研究成果 Cheetah，就数倍地提升了当前安全两方神经网络推理计算的效率，推动了多方安全计算技术在图像识别等复杂模型推理场景的落地。另一种方式是结合 GPU、FPGA、ASIC 等异构硬件能力，提高计算速度。例如，USENIX Security’22

上发布的多方安全计算 GPU 平台 Piranha，通过一系列的适配性调整，解决了 GPU 加速多方安全计算协议的挑战，在现有的 SecureML、Falcon、FantasticFour 协议实现上，相比 CPU 版本提速了数十倍。

在应用扩展方面，当前基于多方安全计算技术实现的应用相对有限，该现象在多方联合统计、查询场景中尤为明显，针对一些复杂的现实业务需求支撑能力有待提升。在 2022 年的安全领域顶级会议 CCS'22 和 CRYPTO'22 中，针对各类现实问题，提出了如支持非唯一连接键的 SQL-join 操作的安全协议和适用于模糊匹配的 PSI 协议，进一步扩展了基于多方安全计算能够实现的应用场景。

（二）联邦学习技术进入快速发展阶段

联邦学习（Federated Learning，FL）是指一种多个参与方在保证各自原始私有数据不出数据方定义的私有边界的前提下，以保护隐私数据的方式交换中间计算结果，从而协作完成某项机器学习任务的模式。根据参与计算的数据在数据方之间分布的情况不同，可以分为横向联邦学习、纵向联邦学习和联邦迁移学习。

联邦学习通过对各参与方间的模型信息交换过程增加安全设计，使得构建的全局模型既能确保用户隐私和数据安全，又能充分利用多方数据，是解决数据孤岛和数据安全问题的重要框架，其强调的核心理念是“数据不动模型动，数据可用不可见”。

2022 年，联邦学习领域涌现出了大量的优秀研究成果。技术创新集中在性能优化、安全加固、模型效用提升等方面。

在性能优化方面，为满足复杂模型训练的实际需求，业内持续探

索高效的联邦学习算法，产出了包括本地多轮迭代、异步协调策略、one-shot 交互协议、压缩等各类技术方案。这些技术方案能够有效降低异构网络、物理距离、通信数据量等因素造成的通信瓶颈的影响，提高模型训练的效率。

在安全加固方面，由于联邦学习需要多方共同参与，开放的环境可能会引入更多的安全风险，并且业内对于联邦学习的安全性证明仍不够充分，技术应用方对于联邦学习安全性的顾虑尚未消除，如何解决联邦学习潜在的安全威胁成为了一大研究热点。近年来，在增强协议的隐私保护能力、抵抗 FL 过程中可能存在的数据泄露、后门攻击等方向均有新方案、新技术的出现，在这些成果的支撑下，联邦学习的安全性正在持续、稳固提升。

在模型效用提升方面，由于联邦学习需要使用多方对齐后的数据进行训练，在参与方数量增加时，交集数据规模可能会随之减少，导致最终训练的模型效果不佳。为解决这一问题，自监督学习、半监督学习、知识蒸馏、迁移学习等 AI 技术都被引入到联邦学习中，以求更有效的发挥可用数据的价值，解决多方交集数据稀缺的问题。

此外，联邦学习为跨组织、跨行业的数据合作提供了新的契机，如何通过技术手段在各方之间建立稳定、可持续的合作关系也成为了联邦学习落地应用时需要解决的问题，诸如**贡献评估、模型可解释性、公平性等研究方向逐渐受到了业内的关注**。

（三） 可信执行环境软硬件均迎来突破

可信执行环境（Trusted Execution Environment，TEE）通过软

硬件方法在中央处理器中构建一个安全的区域，保证其内部加载的程序和数据在机密性和完整性上得到保护。TEE 是一个隔离的执行环境，为在设备上运行的受信任应用程序提供了比普通操作系统更高级别的安全性以及比传统安全元件更丰富的功能。

可信执行环境通过进程级隔离、体系结构层隔离、虚拟化级隔离等技术，为使用者提供一个执行空间，该空间有更强的安全性，且相比常规的安全芯片功能更加丰富，并提供代码和数据的保密性和完整性保护。另外，与纯软件的密码学隐私保护方案相比，TEE 不会对隐私区域内的算法逻辑语言有可计算性方面的限制，其能够支持更多的算子及复杂算法，上层业务表达性更强。利用 TEE 提供的计算度量功能，还可实现运行在其内部的身份、数据、算法全流程的计算一致性证明。

2022 年，可信执行环境技术路线从硬件侧到软件侧均取得了一定进展。

在硬件方面，可信执行环境的技术成熟度不断提升，例如目前应用最为广泛的 Intel SGX 产品逐步更新到第二代，对于计算架构、Enclave 空间大小、内存管理机制、远程认证协议等都有较大幅度的升级。此外，越来越多的硬件产品中都加入了可信执行环境相关能力，国内硬件厂商如海光、兆芯、飞腾、鲲鹏等纷纷推出了集成自研可信执行环境技术的硬件产品，国外知名硬件厂商 Nvidia 也在 2022 年首次将可信执行环境技术融入到了其发布的最新版 GPU 硬件中。

在软件方面，针对可信执行环境技术存在的应用开发难度高、异

构可信硬件隔离等问题，业内开始探索打造更加通用、灵活、适配异构可信执行环境的软件平台。例如，Usenix ATC'22 上发布的通用解决方案 HyperEnclave，就试图通过虚拟化技术来提供统一的 Enclave 抽象，打通各异构可信执行环境平台，进而形成更广阔的应用生态。

（四） 多技术融合，优势互补助力突破应用瓶颈

虽然当前隐私计算正处于快速发展阶段，各主流技术路线的创新与突破层出不穷，但是在短时间内仍然难以从本质上解决单一技术的瓶颈限制，各技术路线都存在着不同的局限性（见表 1）。

表 1 三大主流技术路线整体描述及分析

技术	性能	通用性	安全性	可信方	整体描述	技术成熟度
多方安全计算	低～中	高	高	不需要	通用性高、计算和通信开销大、安全性高，研究时间长，久经考验，性能不断提升	**已达到技术成熟的预期峰值**
可信执行环境	高	高	中～高	需要	通用性高，性能强，开发和部署难度大，需要信任硬件厂商	**快速增长的技术创新阶段**
联邦学习	中	中	中	均可	综合运用 MPC、DP、HE 方法，主要用于 AI 模型训练和预测	**快速增长的技术创新阶段**

为解决单一技术的局限性，多技术融合为解决隐私计算的各类技术瓶颈提供了有效手段。在一些场景下，技术融合往往能够产生“1+1>2”的效果。

多方安全计算与联邦学习融合，借助多方安全计算完成各参与方本地模型的汇聚，增强对中间数据的安全保护能力，实现更加安全的联邦学习聚合算法，如通过秘密分享或全同态加密等方式在密态的环境下完成模型训练。

多方安全计算与可信执行环境融合，借助多方安全计算技术将明文态的数据转为密态后再放入可信执行环境中进行计算，解决可信执行环境所面临的硬件层安全威胁，防止硬件环境被破坏导致的数据隐私泄露。同时，依靠可信执行环境的一系列安全能力，将跨网的多方安全计算节点安全的放置在同一网络内，能够降低多方安全计算通信瓶颈影响，提高效率。

联邦学习与可信执行环境融合，在可信执行环境内完成各类数据的融合计算操作，借助可信执行环境的可信性和隔绝性，保护相关数据的安全与隐私，通过技术手段降低了对可信第三方的信任依赖，增强整套系统的安全性。

在产业实践方面，隐私计算的技术融合应用已经成为一大趋势。根据产品评测实践及市场调研，截至 2022 年 12 月，已通过中国信通院“可信隐私计算”产品评测的 100 余家单位中，38%支持多种不同的隐私计算技术，其中以多方安全计算加联邦学习的占比最高，达到了 33%。

除各主要技术路线之间的融合，零知识证明、差分隐私、区块链等技术也常被应用或辅助于隐私计算。零知识证明能够补充计算过程中对各方计算结果正确性的验证，确保各参与方在计算过程中是诚实的；差分隐私能够作为一种增强数据保护程度的技术手段，与其他隐私计算技术融合应用；区块链一方面能够实现计算全流程可记录、可验证、可追溯、可审计，另一方面可以加强对参与方身份的认证，实现隐私计算任务定向授权验证。

（五） 概念外延，广义隐私计算技术体系形成

近些年，随着全球范围内对于数据安全的重视程度不断增长，隐私计算的应用需求逐渐扩展到了包括数据采集、处理、发布、销毁等全生命周期涉及的所有计算操作，现有定义已无法覆盖这些现实需求，隐私计算的概念逐渐外延。

在欧美，“隐私增强技术”指代有助于遵守隐私或数据保护要求的技术工具或方法，通常与管理措施相结合，包括与信息安全相关的政策和程序、人员管理和访问控制、记录保存和审计等。欧盟网络安全局(ENISA) 将“隐私增强技术”定义为旨在支持数据最小化、匿名化和假名化以及其他核心隐私和数据保护原则的技术。

从国内情况来看，随着隐私计算在应用上的快速发展，为了建立更加完善的隐私计算信任系统，现阶段对于能够促进实现隐私保护和共享数据价值分析的技术方案，均可纳入隐私计算的范畴。隐私计算不再只注重技术和方案的安全性，进而转向了更为全面、完整的保护隐私信息的技术体系，产生了广义隐私计算的概念。

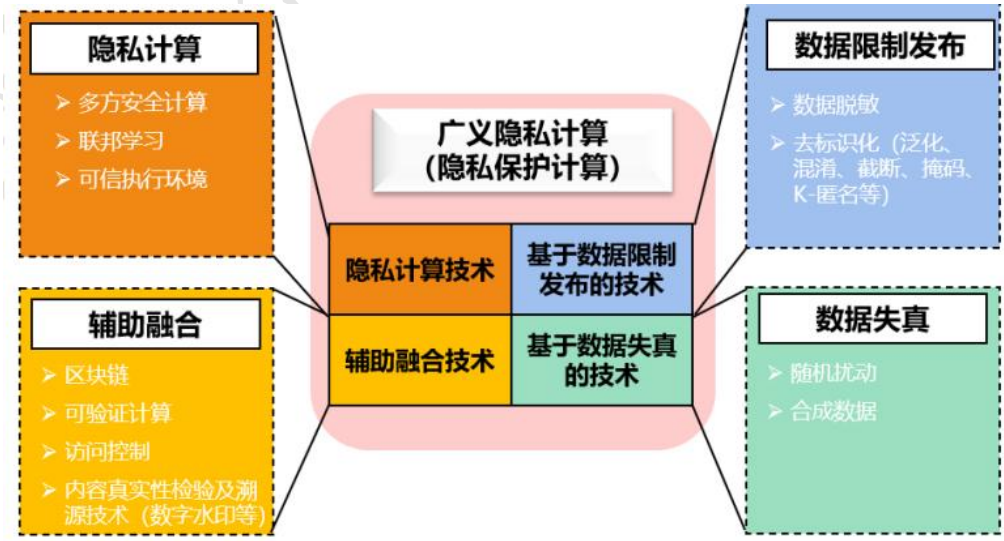

图 2 广义隐私计算技术体系

广义隐私计算是面向隐私信息全生命周期保护的计算理论和方法，涵盖信息所有者、信息转发者、信息接收者在信息采集、存储、处理、发布（含交换）、销毁等全生命周期涉及的所有计算操作，是实现隐私保护前提下数据安全共享的一系列技术。

当前，广义隐私计算技术体系主要包括隐私计算、数据限制发布、辅助融合和数据失真四大类技术（如图 2）。基于数据限制发布和数据失真的技术主要作用于数据发布的前序阶段，能够有效降低原始数据中包含的隐私信息泄露风险。广义隐私计算技术作用于数据的处理、发布阶段，可以实现多方数据融合计算过程的“可用不可见”、“可控可计量”。其他如区块链、可验证计算、访问控制、内容真实性检验及溯源等辅助融合技术为各阶段的验证、追溯、审计提供了有效保障。多种技术融合及技术体系的不断扩展，为隐私计算未来的发展奠定了重要的基础。

三、应用分析

目前，隐私计算在金融、政务、通信、医疗等行业中应用越来越广泛，技术应用的普及范围逐步扩大。大部分应用方虽已对隐私计算有一定了解，但仍比较关心“在诸多业务场景中，隐私计算技术与传统技术方案相比具有哪些优势”。通过调研分析，隐私计算的应用主要覆盖两类场景（如图 3）：**第一类中，**传统信息安全技术已被普遍应用，但仍有安全隐患，隐私计算的应用进一步提升了安全性，我们称为隐私计算存量优化应用场景；**第二类中，**传统信息安全技术无法满足应用需求，隐私计算则提供了解决方案，拓展了数据安全流通的

应用场景，我们称为隐私计算增量创新应用场景。下文将聚焦这两类隐私计算场景进行详细论述。

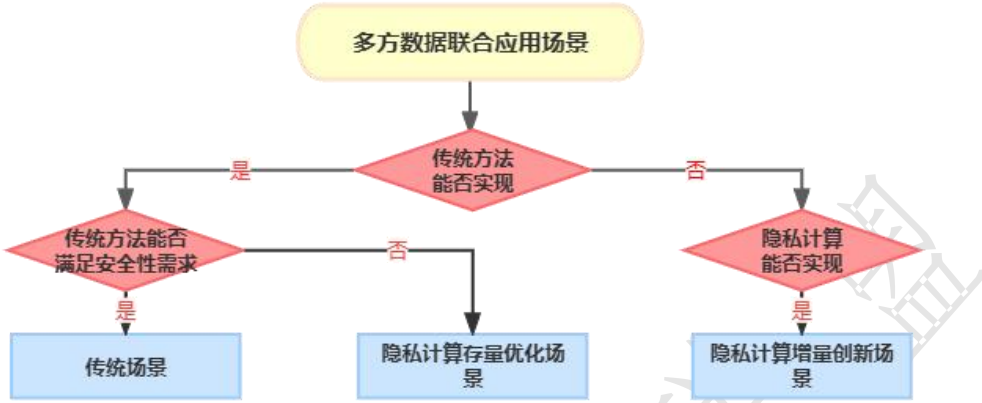

图 3 隐私计算应用覆盖场景示意图

（一） 存量优化，隐私计算提升传统场景安全

传统信息安全技术可以一定程度上实现数据的安全流通和共享利用，但是在数据传输过程中存在着较大的原始数据泄露风险、在数据使用过程中存在着滥用挪用风险。虽然通过加强事前风险控制设计、事后退出及审计等方式可以在一定程度上降低上述风险概率或减轻损失，但是需要花费大量的沟通及监督管理成本，效果也往往不尽如人意。

隐私计算在技术层面提升数据流通安全性，实现数据的**“可用不可见”**，有效降低原始数据泄露风险。同时，隐私计算能够使得数据提供方实现对其每一个数据集以及每一个计算任务的感知化、精细化管理，从技术层面最大化避免滥用挪用风险。

因此，在传统数据流通技术应用较为普遍的场景中，隐私计算为

各合作方的数据安全提供了更加有效的保护，这类场景的特点如下：**一是**受政策、监管要求，原始数据保护要求较为严格；**二是**在保护原始数据安全下，通过共享数据 ID 提高计算效率。通过隐私计算技术在数据联合分析、数据隐私求交、数据联合建模预测等数据利用场景中，基于通信信道加密、哈希加密、算法加密以及其他加密手段保证各参与方原始数据的安全；**三是**合作方数据集规模较大，往往数倍于发起方，这种数据量上的不平衡导致发起方希望根据真实参与计算的数据来评估数据价值。

通过研究不同隐私计算存量优化应用场景案例（见附录 1）特点，提炼出隐私计算存量优化应用场景通用解决方案模型（如图 4）：

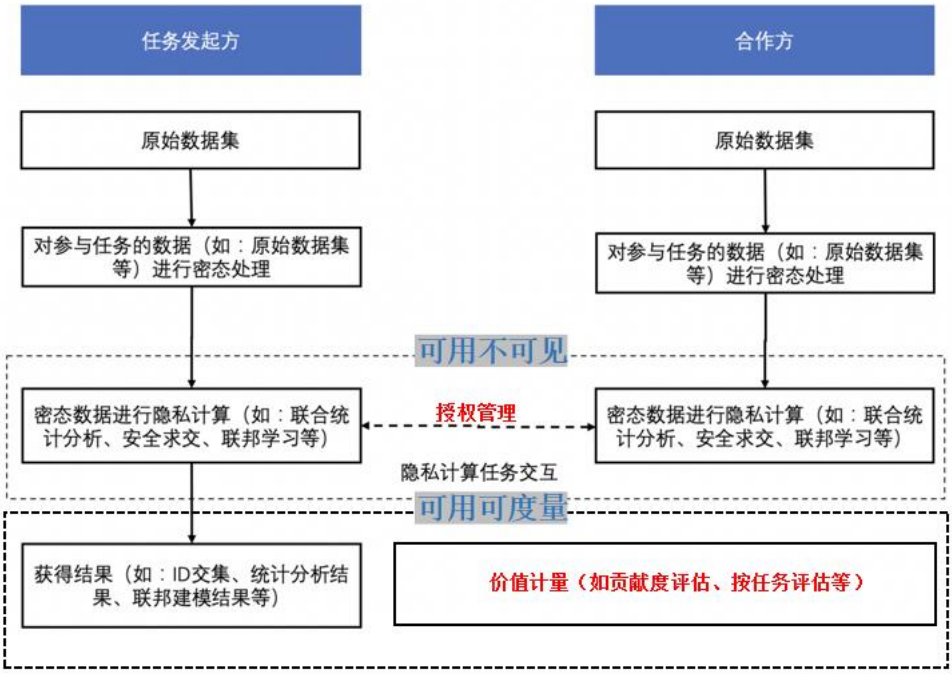

图 4 隐私计算存量优化应用场景通用解决方案模型

专栏 1：基于隐私计算的联合营销及客户运营优化解决方案

银行机构在精准营销应用场景中，对于数据安全以及相关技术的落地要求进一步提高。不仅需要实现数据可用性和安全性的科学平衡，又需要覆盖法律、管理、业务、技术等专业领域。为提高传统合规模式的安全性，隐私计算技术成为关键路径。

本案例通过隐私计算技术，为银行安全、高效地拓展了通信运营商和互联网渠道商的高价值外部数据，实现了优质新客拓展、潜客精准投放和客户线下运营三大经典金融场景的有机串联，补充了以往仅依靠自身数据无法补全的客户画像缺失碎片，增加了内外部可合作的业务场景丰富度，为客户带来了更好的全生命周期体验。

图 A 基于隐私计算的联合营销及客户运营优化

以上多场景串联隐私计算合作模式，在优质新客拓展阶段实现了外呼接通率上升 15%、申请通过率提升 2%的好成绩，在潜客精准投放阶段累计拓展新增用户超 1 万人、降低总营销成本近 10%，在客户线下运营阶段，网点单日引流人数较以往提升约 40%，期间为满足营销活动要求的客户提供了各种权益和关怀手段，大幅提升了客户满意度和客户粘性，实现了三个营销场景的有机串联。

专栏 2：基于隐私计算的传染病多点触发监测及预警解决方案

由于传染病的防控涉及大量个人数据、传染病临床数据等高度隐私敏感数据，传染病数据平台需要强大的安全权限保护以防止数据泄露问题。另一方面传染病的防控研究涉及到很多医学、统计、AI 等不同的专业知识，需要不同类型的专业工作者，多方共同参与使用这些数据来研究难题。因此只有通过隐私计算技术才能解决在确保数据安全、个人隐私、数据授权使用的前提下让数据高效流通起来的难题。

某城市通过隐私计算技术实现在数据安全、授权、隐私保护的前提下建立开放数据协作机制，联动了卫生健康部门以及海关、边防、民航、教育、市场监管、商务、交通、民政、公安、通信、住建等政务部门的数据。通过联邦学习，构建涵盖人员、物品及产品、环境及场所的全面智慧化预警多点触发机制，完善传染病疫情监测系统，织密不明原因疾病、聚集性病例和异常健康事件的监测网。

通过传染病多点触发监测和智慧化预警平台建设，完善传染病疫情监测系统，实现病例和症状监测信息直接抓取、实时汇集，提高疫情实时分析、集中研判的能力。智慧化预警平台有效预警高达 700 次/月，法定传染病网络直报运行率为 100%，医疗机构传染病漏报率城区低于 2%、县市低于 4%。通过使用数据治理应用，对于自然语言描述的医疗主观数据进行结构化处理，大大减少了人工投入，建立持续地数据治理流程，效率比传统方法提高 10 倍以上，通过哨点监控辅助诊断 1 万次/月，症候群预测准确率达到 88%。

（二）增量创新，隐私计算满足新兴场景需求

除传统数据流通应用场景之外，新兴应用场景涌现并对数据流通技术提出了新的要求。在这些场景中，数据流通合作中发起方数据集ID包含个人隐私数据，随着法律和监管的要求提高，发起方产生保护本方数据集ID的需求。这种场景下，传统数据流通应用模式如文件交换、系统对接、接口调用等难以实现。而隐私计算通过其独有的隐匿查询、全匿踪求交等方式，新增在不暴露数据ID的同时完成联合查询、联合建模等任务的能力，扩展了传统数据流通合作保护范围，补全了数据全生命周期保护中最困难的一环，成为满足新兴应用场景需求的开拓者。

隐私计算增量创新应用场景主要包含以下特点：**一是**受政策、监管要求，原始数据保护要求严格；**二是**在保护原始数据安全的同时，在安全可控等方面具有特殊的要求，如需要在保护数据ID的条件下完成特定计算任务；**三是**传统信息安全技术无法满足新兴场景要求，但隐私计算利用其技术优势能够满足要求。通过研究不同隐私计算增量创新应用场景案例（见附录2）特点，提炼出隐私计算增量创新应用场景通用解决方案模型（如图5）：

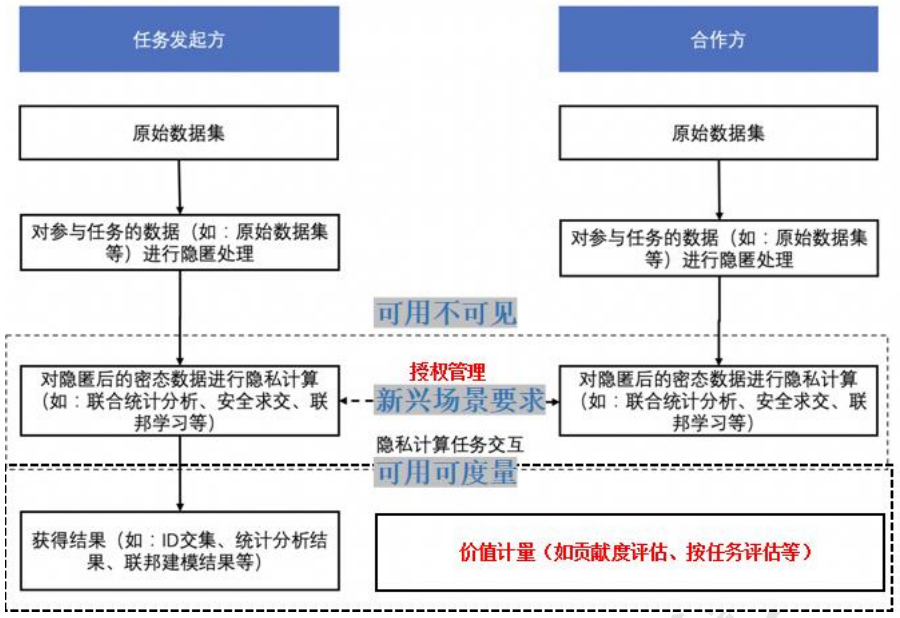

图 5 隐私计算增量创新应用场景通用解决方案模型

由于增量创新应用场景范围较广，下文以一个典型增量创新场景举例详细阐述。该场景下，新兴场景要求为在不暴露明文 ID 的条件下与合作方完成联合查询和联合建模。传统信息安全技术无法实现该要求，但隐私计算通过其独有的隐匿查询、全匿踪求交等方式能够实现该场景。此时，该场景解决方案模型（如图 6）：

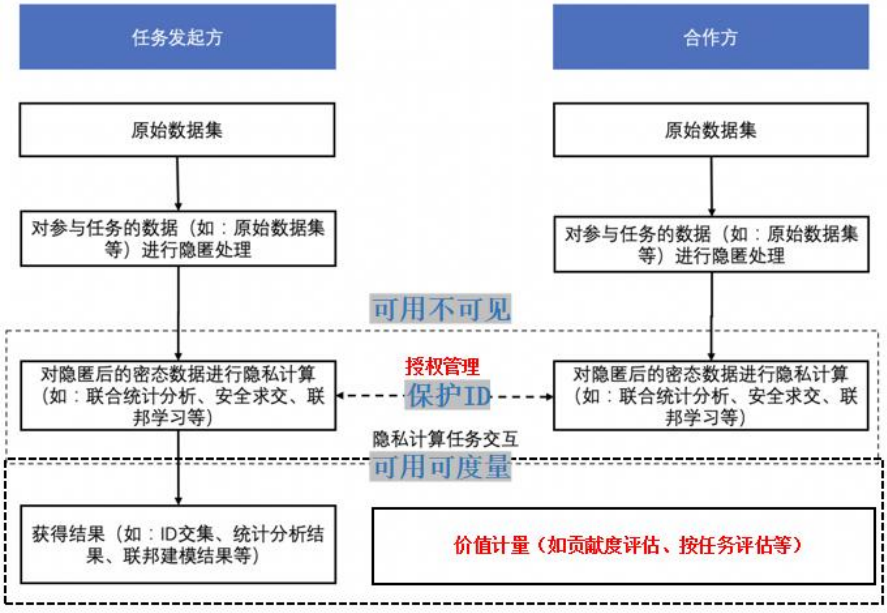

图 6 隐私计算不暴露明文 ID 解决方案模型

该场景主要包含两种情况，其一是通过隐匿查询可获得结果的场景，其二是以全匿踪求交作为前置步骤并通过联合统计、联合建模预测等方式获得结果的场景。隐匿查询中，既保护了查询目标以外其他数据的安全，又保护了查询目标用户的 ID；全匿踪求交中，既保护了所有数据的特征信息和非交集部分的用户 ID，又保护了数据求交时交集部分的用户 ID。

专栏 3：基于全匿踪联邦学习的反电信欺诈解决方案

目前多数据方联合反诈场景中，有新兴场景提出“不泄露交集 ID”的需求。此时，传统的数据流通技术无法解决这一场景问题。通过使用支持不暴露交集和非交集用户任何个人信息、支持多种数据场景的隐私计算“全匿踪联邦学习”技术，可实现电信网络诈骗风险预警模型构建。

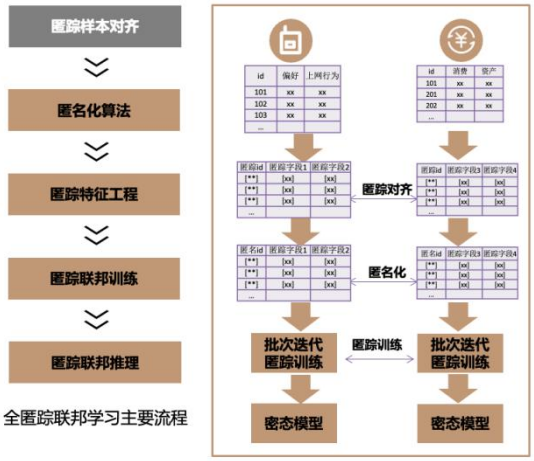

图 B 基于全匿踪联邦学习的反电信欺诈解决方案示意图

目前利用“全匿踪联邦学习”技术可以实现以下 2 个场景应用示范：一是账户反电诈场景，通过身份证匿踪查询某运营商电诈风险名单库（此库包含公安下发的电诈黑名单库），在银行作为灰名单使用。二是对转账用户受诈识别，通过某运营商受电诈名单库及受诈模型分析识别受害者风险，输出是否受诈用户及受诈评分。

反电诈场景应用“全匿踪联邦学习”后效果显著，当前已完成试点应用，即将进入生产环境落地阶段。在联合某银行和某运营商的账户反电诈场景中，使用全国范围内的数万个样本，覆盖 40%电诈用户，准确率高达 91.35%，成功实现电诈账户率下降 30%。

专栏 4：基于改进隐私计算的用户三要素核验解决方案

核验用户基础信息的真实性可以通过查询公安、社保及征信等相关部门的数据库中用户姓名、身份证号、手机号、工作单位和地址等信息。由于这些数据属于用户高度敏感数据和个人隐私数据，相关部门对这些数据的开放持谨慎态度。金融机构在查询用户基本信息时希望避免留下带有被查询用户的记录，以防用户信息泄露。

传统的三要素核验，大都是基于 API 接口的形式，金融机构每次核验查询的信息会以日志的形式记录于服务器中，容易造成数据泄露。基于隐私计算的用户三要素核验，对隐私求交模块进行优化，使之在隐私求交之后不为双方返回交集内容，而是向业务需求方返回是否有交集的布尔值，这样数据需求方不会暴露查询内容，而数据源方也不会有数据泄露的风险，双方业务不存在敏感数据的传输，输出内容仅仅表示是否正确的布尔值。

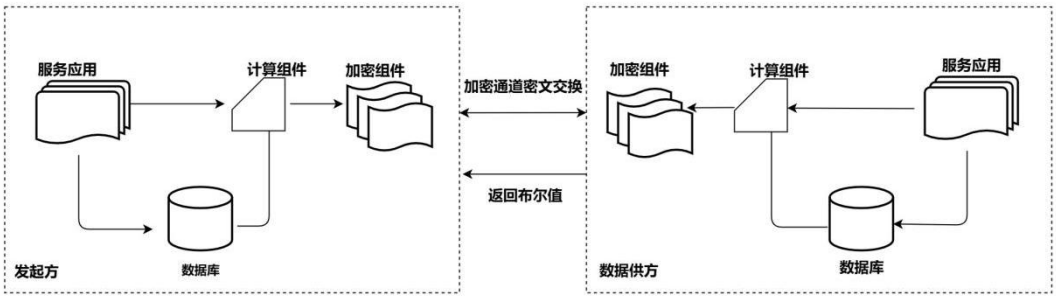

图 C 基于改进隐私计算的用户三要素核验解决方案示意图

该场景下，各方可部署隐私计算平台产品，也可部署相关组件应用的轻量级产品，双方经过网络联调和小样本 POC 测试完成，即可开展生产应用。基于双方数据的量级可以实施相应的数据加工策略，比如分桶处理后再逐桶完成 PSI 任务，有效提升计算效率。

四、行业分析

隐私计算近几年发展迅速，产品数量迅速增长，研究成果不断产出，技术逐渐成熟，加上开源技术的普及和相关标准的落地，隐私计算进一步规范化。当前，隐私计算行业已步入产业增长阶段，应用规模稳步增长，业务范围不断拓展。在未来，随着政策完善与技术进一步发展，隐私计算市场将会更加广阔。

（一）隐私计算供需双方共建产业生态

从现有应用来看，隐私计算主要服务于机构之间的数据流通，即以 To B 市场为主。应用方往往通过自建或采购技术平台服务的方式，将隐私计算应用于保护自有数据资源地安全流通与应用。因此，从产业生态构成看，根据 2022 年 9 月隐私计算联盟发布的《隐私技术产业图谱 1.0》，隐私计算产业构成主要可分为行业应用需求方、隐私计算技术提供方等主体，其中技术提供方又包含软件、硬件提供商等。

行业应用需求方随技术应用的深入不断拓展范围。行业应用需求方需要使用隐私计算技术来解决自身业务开展中数据应用所带来的风险与安全问题。从业务性质上，行业应用需求方可进一步分为数据提供方与数据应用方。数据提供方一般通过企业内部业务积累、企业外部定向采购、定制化采集等方式汇聚大量数据，在进行加工处理后，形成可对外提供的数据产品或服务，实现自身持有的数据资源的商业化变现。而数据应用方则是在业务发展过程中产生了数据应用的资源缺口，需要引入外部数据资源来为自身的业务场景做技术加持。随着数字化转型的深入和数智化应用的拓展，各类企业内外部数据融合应

用的意识逐步提升，数据流通的需求不断增强，目前，隐私计算的行业应用需求方已覆盖金融、政务、通信、互联网、医疗、工业以及能源等多个行业。其中，技术能力基础较好的企业，也开始拓展业务范围、搭建自身的隐私计算产品以及平台，并向隐私计算技术提供方的方向拓展。

隐私计算已成为数据技术服务领域的热门赛道。隐私计算技术提供方主要通过自研或开源的技术框架，实现了以多方安全计算、联邦学习、可信执行环境为主要技术路线的隐私计算平台类产品。隐私计算技术提供方与行业应用需求方之间互动紧密，通过部署隐私计算节点到数据提供方与数据应用方，一方面解决了以往数据使用时数据出域、数据泄露等安全隐患，另一方面提升了具体业务场景的效果。在政策支持和市场需求的双重推动下，隐私计算技术提供方从大型科技集团和创业企业，逐渐扩展到包括隐私计算垂直企业、综合科技类企业、大数据企业、金融科技企业、AI 服务企业、区块链企业、云服务企业、信息安全企业等多类企业在内的产业格局。不同类型的隐私计算技术提供方在技术、服务和商业资源等方面各具初始优势，但随着产品成熟度的提升，产品功能的竞争差距逐步缩小，配套的服务能力和数据应用、运营能力或将成为未来隐私计算技术提供方的主要竞争点。

硬件支持方也属于隐私计算技术提供方，为隐私计算应用提供关键支撑。硬件支持方对于隐私计算产业乃至数据要素产业都有着非常重要的意义，无论是数据存储、数据治理、数据分析还是数据计算都

离不开硬件的相关支持。在隐私计算领域，硬件支持方与隐私计算技术提供方的合作尤为密切，目前出现的隐私计算一体机包含了可信执行环境、密码卡等提升安全，也通过 GPU、FPGA 等进一步加速性能。近几年，国内企业也开始加速隐私计算领域的核心硬件研发。

（二） 隐私计算未来市场整体前景广阔

隐私计算作为处于产业快速增长期的新兴行业，其市场规模一直受到各研究机构的广泛持续关注。目前，对于隐私计算市场规模的统计口径从亿级到百亿级不等，但整体来看，各方观点均认为面向服务数据要素的流通和价值释放，隐私计算市场前景广阔。以 Gartner 为代表，其在《2022 年重要战略技术趋势》中预测“到 2025 年 60%的大型企业机构会在分析、商业智能或云计算领域采用一种或多种隐私计算技术”，对隐私计算的市场普及渗透率提升持积极态度。表 2 为部分机构在相关成果中公开的国内隐私计算市场规模测算结果。

表 2 我国隐私计算市场规模的相关测算结果

发布时间	发布单位	发布渠道	测算结果
2021 年 4 月	微众银行、毕马威	《深潜数据蓝海：隐私计算行业研究报告》	国内市场规模将快速发展，三年后技术服务营收有望触达**100-200 亿**人民币的空间，甚至将撬动千亿级的数据平台运营收入空间
2021 年 12 月	甲子光年	《2021 年中国隐私计算市场研究报告》	**2025 年**整体市场规模超**200 亿元**，2021-2025 年 CAGR 超 100%

发布时间	发布单位	发布渠道	测算结果
2022 年 4 月	IDC	《IDC Perspective: 隐私计算全景研究》	隐私计算系统/软件销售与服务收入在 **2025 年**规模可达 **350 亿 ~ 700 亿**元，通过隐私计算平台上产生的业务运营分润收入可以达到 5600 亿元
2022 年 4 月	艾瑞咨询	《2022 年中国隐私计算行业研究报告》	**2021** 年中国隐私计算市场规模为 **4.9 亿元**，预计至 **2025 年**将达到 **145.1 亿元**，数据运营占比持续升高
2022 年 5 月	国家工业信息安全发展研究中心	《中国隐私计算产业发展报告（2020-2021）》	隐私计算产品市场规模约为**十亿元**，基于隐私计算的数据交易应用模式市场或将达到千亿级。
2022 年 10 月	亿欧智库	《2022 中国隐私计算产业研究报告》	**2021 年**隐私计算产品市场规模约为 **10 亿元**，**2025 年**预计为 **192.2 亿元**
2022 年 11 月	PCview 隐私计算研究院	《2022 年中国隐私计算行业洞察报告》	中国隐私计算行业将迎来快速增长，预计至 **2026 年**市场规模将达 **184 亿元**，年复合增长率为 103.3%

可以看到，国内隐私计算市场规模的测算方法还没有形成行业普遍认可的共识。我们认为，这需要从隐私计算技术提供方现有的商业模式入手进行分析。根据调研，目前隐私计算技术提供方的商业模式可分为平台建设与数据运营两类。平台建设是指提供软件产品、技术服务和解决方案等服务，按项目计费；数据运营是指基于隐私计算平台开发数据增值产品、建立数据智能模型、服务不同客户场景产生的平台性运营分润收入（具体包含按数据使用量分润或按业务效果分润）。

两类商业模式的市场增长空间，决定了隐私计算未来的整体市场

规模。平台建设的市场空间增长驱动因素以行业扩展为主、中长尾客户（即客单价相对较小的客户）延伸为辅，在现有的金融、通信、政务三大核心行业的基础上，医疗、能源、广告、交通等行业有望拓展更多客户。数据运营的市场空间增长驱动因素来自于两方面，一是传统数据流通模式的重构，例如，从传统数据集或 API 调用向隐私计算模式进行升级改造；二是可流通数据资源范围的扩大，例如，政务数据开放中很多无法直接开放的高价值敏感数据有望通过隐私计算技术面向社会提供给开发利用机会。**从两类商业模式市场增长驱动因素出发，结合相关数据进行分类测算，我们预计到 2025 年我国隐私计算市场规模将达到百亿元。**

（三） 隐私计算领域科研成果快速增长

1.标准情况

技术应用需要统一的标准规范划定基线，随着隐私计算技术不断落地应用，标准研制工作也在紧锣密鼓地开展。从 IEEE、ISO、ITU-T 等国际标准化组织到中国通信标准化协会（CCSA）、全国金融标准化技术委员会（金标委）等国内组织都在积极组织行业专家制定隐私计算相关标准。

国际标准开始向安全和应用扩展。除了最早密码学技术（同态加密、秘密分享等）的国际标准，各个国际组织从 2018 年开始陆续启动隐私计算技术标准的制定工作。目前框架类、功能类标准已经发布，对多方安全计算、联邦学习的安全要求标准、技术应用类标准（如互联互通、一体机）也在编制过程中，如表 3 所示。

表 3 隐私计算国际相关标准情况

组织	标准名称	状态	发起单位
IEEE	P3652.1《IEEE Guide for Architectural Framework and Application of Federated Machine Learning》（联邦学习架构框架与应用指南）	2018 年立项 2021 年发布	微众银行
	P2842《Recommended Practice for Secure Multi-Party Computation》（多方安全计算参考框架）	2019 年立项	阿里巴巴
	P2830《Standard for Technical Framework and Requirements of Trusted Execution Environment based Shared Machine Learning》（基于可信执行环境的共享机器学习技术框架和要求）	2019 年立项	蚂蚁集团
	P2952《Standard for Secure Computing Based on Trusted Execution Environment》（基于可信执行环境的安全计算）	2020 年立项	蚂蚁集团
	P2986《Recommended Practice for Privacy and Security for Federated Machine Learning》	2021 年立项	中国电信
	P3156《Standard for Requirements of Privacy-preserving Computation Integrated Platforms》（隐私计算一体机技术要求）	2022 年立项	蚂蚁集团
	P3117《Standard for Interworking Framework for Privacy-Preserving Computation》（隐私计算互联互通框架）	2022 年立项	洞见科技
	P3169《Standard for Security Requirement of Privacy-preserving computation》（隐私计算安全要求）	2022 年立项	蚂蚁集团
ISO/IEC JTC1 SC27	ISO/IEC 19592-1《Information technology - Security techniques - Secret sharing》(信息技术-安全技术-秘密分享)	2016 年发布	——
	ISO/IEC 18033-6《Information technology - Security techniques - Encryption algorithms - Part 6 : Homomorphic encryption》（信息技术-安全技术-加密算法-同态加密）	2019 年发布	——
	ISO/IEC 4922-1《Information security - Secure multiparty computation - Part 1: General》（信息安全-多方安全计算-第 1 部分：通用）	2020 年立项	德国标准化学会
	ISO/IEC 4922-2《Information security - Secure multiparty computation - Part 2: Mechanisms based on secret sharing》（信息安全-多方安全计算-第 2 部分：基于秘密分享）	2020 年立项	德国标准化学会
ITU-T	F.748.13《Technical framework for a shared machine learning system》（共享学习系统技术框架）	2021 年发布	蚂蚁集团
	《Management Requirements for Federated Machine Learning Systems》（联邦学习管理能力要求）	2021 年立项	北京邮电大学
	X.1770《Technical guidelines for secure multi-party	2021 年发布	阿里巴巴

组织	标准名称	状态	发起单位
	computation》（多方安全计算技术指南）		
	《Assessment Criteria for Federated Learning Platforms》（联邦学习平台评估方法）	2022 年立项	中国信通院

国内标准开始迈入应用场景。相比国际标准，国内隐私计算相关标准迭代更快，已经从技术产品的功能、性能、安全向着应用场景、软硬结合等方向扩展。中国通信标准化协会大数据技术标准推进委员会（CCSA TC601）自 2018 年开始制定隐私计算领域的相关标准，由中国信通院云大所、隐私计算联盟牵头联合业内单位，已经构建了可信隐私计算标准体系，包含产品基础能力、性能、安全、互联互通和各类行业场景应用等系列标准。此外，全国信息技术标准化技术委员会（TC28）、全国信息安全标准化技术委员会（TC260）、全国金融标准化技术委员会（TC180）等组织和单位，各方也在各自领域内统筹规划和稳步推进相关标准。国内相关标准如表 4 所示。

表 4 隐私计算国内相关标准情况

组织	标准名称	标准类别	进展
中国通信标准化协会	《基于多方安全计算的数据流通产品 技术要求与测试方法》	功能	已发布
	《基于联邦学习的数据流通产品 技术要求与测试方法》	功能	已发布
	《基于可信执行环境的数据计算平台 技术要求与测试方法》	功能	已发布
	《区块链辅助的隐私计算技术工具 技术要求与测试方法》	功能	已发布
	《隐私计算 多方安全计算产品性能要求和测试方法》	性能	已发布
	《隐私计算 联邦学习产品性能要求和测试方法》	性能	已发布
	《隐私计算 可信执行环境产品性能要求和测试方法》	性能	已发布
	《电信网和互联网联邦学习技术要求与测试方法》	性能	制定中
	《隐私计算 多方安全计算产品安全要求和测试方法》	安全	已发布
	《隐私计算 联邦学习产品安全要求和测试方法》	安全	已发布
	《隐私计算 可信执行环境产品安全要求和测试方法》	安全	已发布
	《隐私计算安全部署环境技术要求》	安全	制定中
	《隐私计算应用 面向金融场景的应用要求》	应用	已发布
	《隐私计算应用 面向政务场景的应用要求》	应用	制定中
	《隐私计算应用 面向互联网场景的应用要求》	应用	制定中
	《隐私计算应用 面向通信场景的应用要求》	应用	制定中
	《联邦学习业务质量评估方法》	应用	制定中

组织	标准名称	标准类别	进展
	《隐私计算应用一体机技术要求》	服务	制定中
	《隐私计算 跨平台互联互通》系列标准	互联	制定中
全国信息安全标准化技术委员会	《信息安全技术 机密计算通用框架》	功能	制定中
	《隐私计算技术应用指南》	应用	制定中
	《隐私保护的数据互联互通协议规范》	互联	制定中
全国金融标准化技术委员会	《多方安全计算金融应用技术规范》	应用	已发布
	《联邦学习金融应用技术规范》	应用	制定中
中国人工智能产业发展联盟	《共享学习系统技术要求》	功能	已发布
中国互联网协会	《金融场景隐私保护计算平台技术要求与测试方法》	应用	已发布
中国支付清算协会	《多方安全计算金融应用评估规范》	应用	已发布
注：以上信息统计时间截至 2022 年 10 月			

2.论文、专利等情况

作为一种新兴的融合技术，隐私计算的理论研究和技术应用产出均呈现上升趋势，这与世界各国重视数据隐私安全的政策基调一致（如图 7）。统计截止到 2022 年 11 月，根据论文作者所在机构所属国家进行排序（如图 8），发现近五年来，隐私计算论文发布量 TOP10 国家是中国、美国、印度、澳大利亚、日本、加拿大、英国、德国、韩国、法国，相关论文量较突出的国家是中国（5121 篇）和美国（4899 篇）。

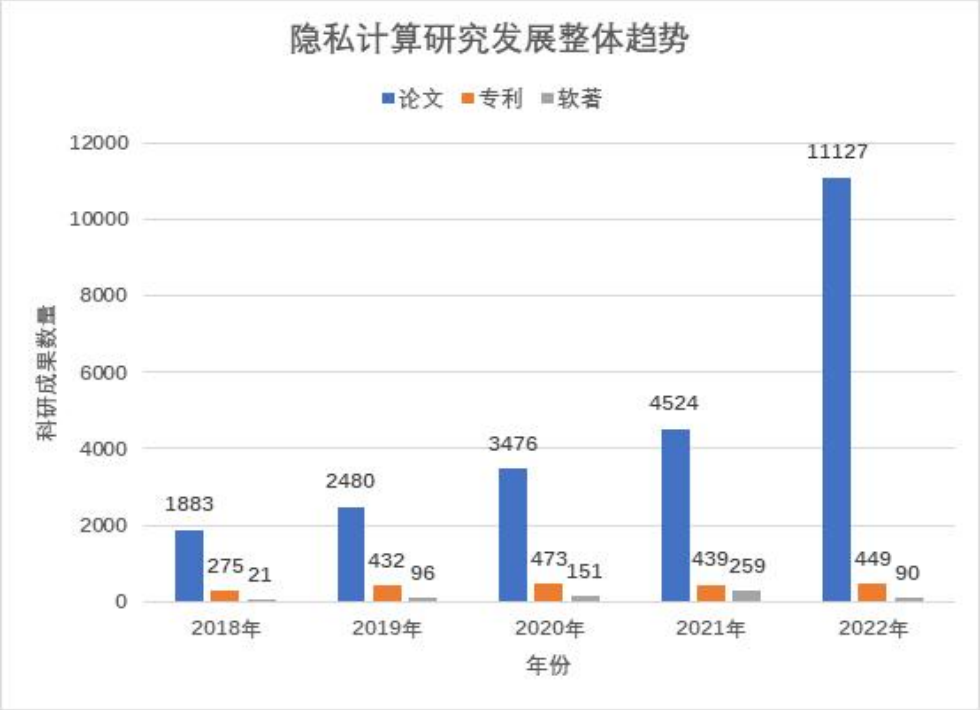

图 7 近五年隐私计算科研成果（论文、专利、软著）统计

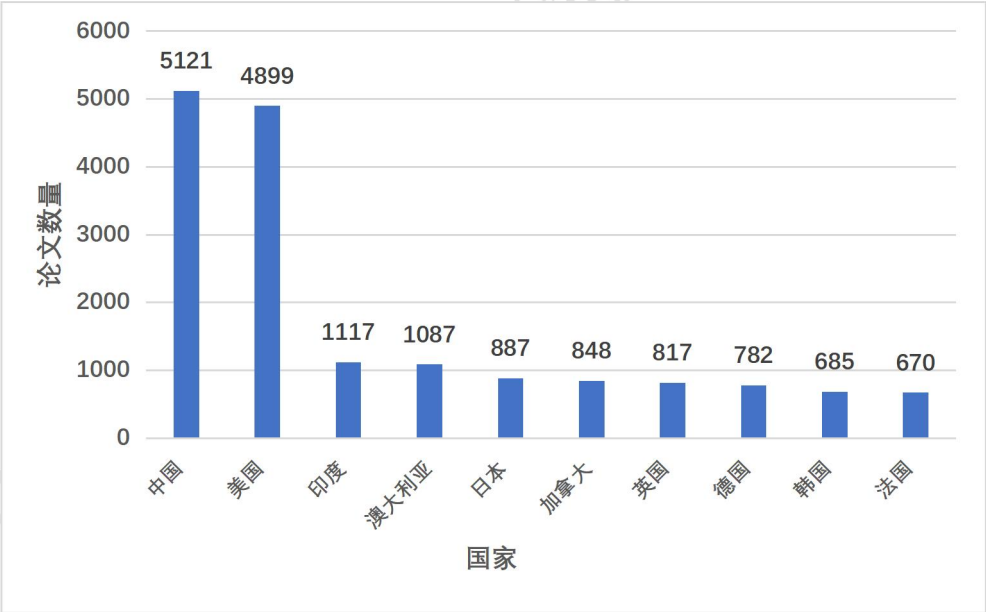

图 8 各国隐私计算领域论文发表数量（Top10）（2018-2022）

从科研成果来看，不同技术的科研产出分布存在显著差异。截止到 2022 年 11 月，在论文方面（如图 9），联邦学习、差分隐私、可信执行环境发表和引用数量最多；在专利方面（如图 10），联邦学

习和可信执行环境公开和授权数量最多；在软著方面（如图 11），联邦学习和多方安全计算转换成果最多。综合来看，多方安全计算技术较为成熟，联邦学习、可信执行环境、差分隐私的研究处于技术爬升期，其中联邦学习的研究增速最快。

从技术研究现状来看，各技术的发展阶段和研究热点也略有不同。多方安全计算理论研究相对较少，专利和软著增速较为平缓，更侧重与云计算、移动计算、区块链、物联网等应用领域结合。联邦学习处于技术“创新触发期”，论文、专利和软著呈现指数增长状态，发表论文数量众多且受到顶级期刊 Nature、Science 的青睐，当下热点包括数据和系统异质性、降低通信开销、提升模型精度等。可信执行环境的国内专利数量已经超过海外专利总量，软著数量呈现快速上升趋势，表明国内企业积极布局 TEE 的软硬件研发，目前主要研究如何实现支持大规模计算或数据密集(CDI)计算方案。

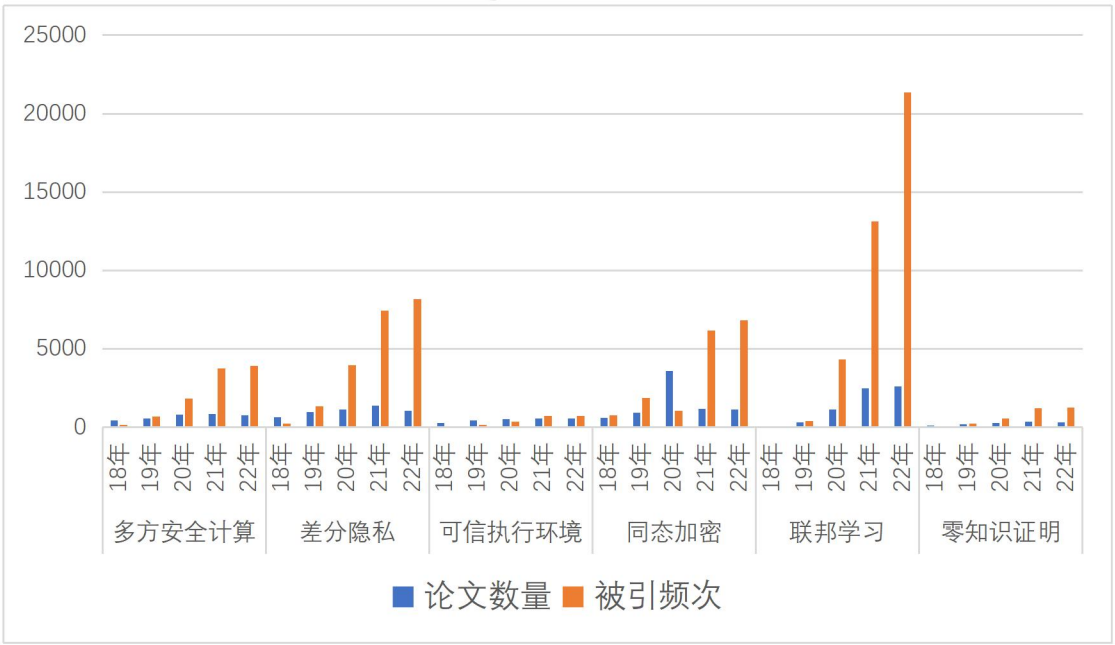

图 9 隐私计算研究论文近五年发展趋势（2018-2022）

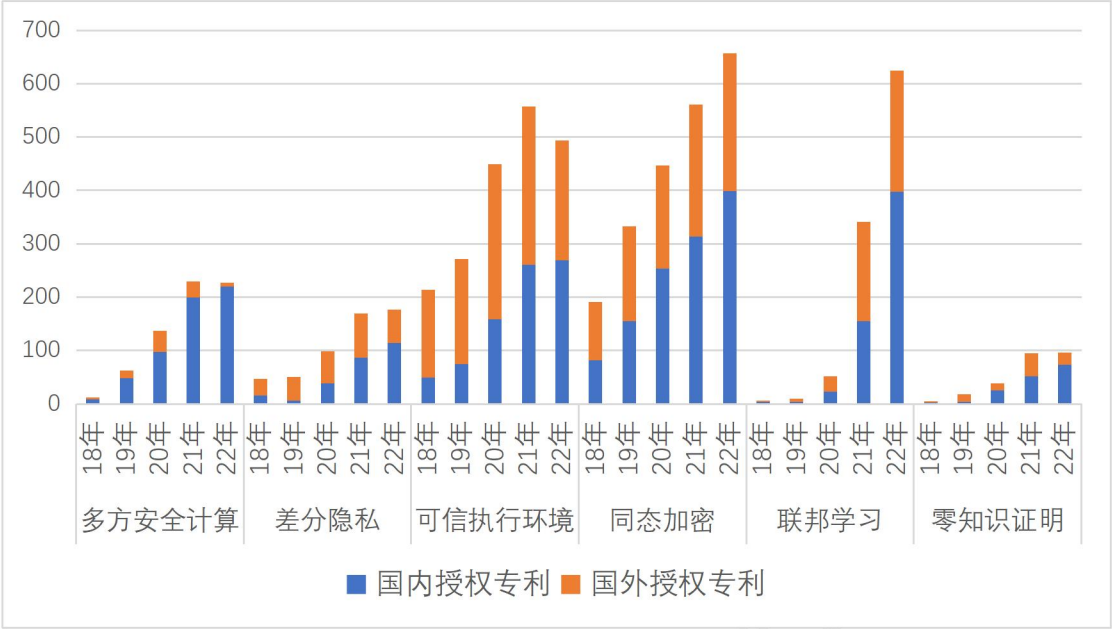

图 10 隐私计算海内外专利近五年发展趋势（2018-2022）

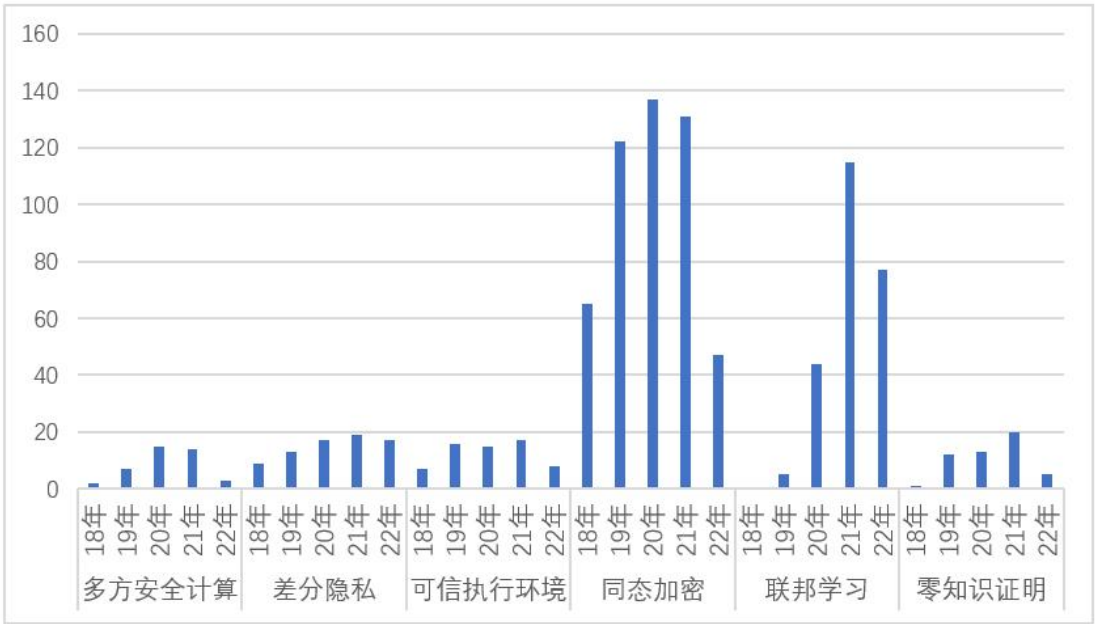

图 11 隐私计算国内软著近五年发展趋势（2018-2022）

（四） 开源促进隐私计算行业蓬勃发展

2021 年 3 月，“开源”一词首次纳入国家《“十四五”规划和 2035 年远景目标纲要》，同年 11 月工业和信息化部发布《“十四五”软件和信息技术服务业发展规划》指出要繁荣国内开源生态，大力发展国

内开源基金会等开源组织，完善开源软件治理规则，普及开源软件文化，加快建设开源代码托管平台等基础设施。随着政策鼓励与技术进步，开源作为一种新型的生产协作方式正逐渐融入到各个技术领域。

开源对于隐私计算行业发展同样具有借鉴意义。一方面，开源降低隐私计算行业的门槛，为行业发展带来活力。企业可以基于隐私计算开源项目快速部署和开发自有的隐私计算平台，缩短开发周期，短期内形成大量的隐私计算产品和行业应用。众多的开发与应用同时可以反哺隐私计算开源平台，进一步促进技术和平台功能的迭代。另一方面，开源提升隐私计算平台安全可信性。可信和安全是隐私计算行业的重要诉求，开源社区的环境公正、代码公开和过程公开等特点使得用户对开源项目更易信赖，同时，由于平台代码对任何人开放，用户可以检验和监督平台的安全性，项目中潜在的安全风险更易被发现和解决。

国内外隐私计算开源项目持续涌现，为行业带来更多选择。从2017年至今主要的开源项目已有数十余个（如表5）。从项目数量上来看，相比去年，今年开源项目的数量翻一倍。技术路线依然集中在多方安全计算和联邦学习，可信执行环境的开源项目在2018年和2019年出现较多。隐私计算开源项目从性质来划分有以下几类：第一类是底层协议相关项目，这一类通常以提升算法性能和安全性为目标，包含多种算法，并通常可以嵌入其他平台；第二类是产品平台类项目，突出产品易用性和功能完备性，用户可以快速上手和使用隐私计算系统；第三类是针对应用场景的解决方案类开源项目，支持多样的应用场景，

并方便用户快速开展应用。

隐私计算开源项目逐渐成熟，助力行业高质量发展。随着近几年技术发展，隐私计算开源项目相较之前更加安全和易用，功能也更完善。从开源项目的 GitHub 热度来看（截至 2022 年 10 月），影响力最高的是集成了联邦学习、差分隐私、多方安全计算等技术的主要用于深度学习框架的 PySyft，Star 数 8300，Issue 数超 3000；排名第二的是 FATE 联邦学习开源平台，Star 数 4500，Issue 数超 6000。另外，TF-Federated、CrypTen 和 SecretFlow 项目热度也较高，Star 数均过千。此外，成熟的开源社区吸引越来越多的开发者参与，众多开发者的交流和贡献也为隐私计算行业发展增添了活力。

表 5 目前国内外主要的隐私计算开源项目

序号	项目名	开源时间	发起机构	技术路径
1	PySyft	2017 年 7 月	OpenMined	多方安全计算、联邦学习
2	TF-Encrypted	2018 年 3 月	DropoutLabs、Openmined、阿里巴巴	多方安全计算
3	EzPC	2018 年 4 月	微软	多方安全计算
4	Asylo	2018 年 5 月	谷歌	可信执行环境
5	Apache Teaclave (incubating)	2018 年 9 月	百度	可信执行环境
6	FATE	2019 年 2 月	微众银行	联邦学习
7	Occlum	2019 年 3 月	蚂蚁集团	可信执行环境
8	TF-Federated	2019 年 8 月	谷歌	联邦学习
9	Private Join & Compute	2019 年 8 月	谷歌	多方安全计算
10	PaddleFL	2019 年 9 月	百度	联邦学习
11	CrypTen	2019 年 10 月	Facebook	多方安全计算
12	Fedlearner	2020 年 1 月	字节跳动	联邦学习
13	Rosetta	2020 年 8 月	矩阵元	多方安全计算
14	KubeTEE	2020 年 9 月	蚂蚁集团	可信执行环境
15	Fedlearn	2021 年 7 月	京东科技	联邦学习
16	WeFe	2021 年 10 月	天冕科技	联邦学习
17	OpenCheetah	2022 年 3 月	阿里巴巴	多方安全计算

序号	项目名	开源时间	发起机构	技术路径
18	FederatedScope	2022 年 5 月	阿里巴巴	联邦学习
19	Primihub	2022 年 5 月	原语科技	多方安全计算
20	SecretFlow	2022 年 7 月	蚂蚁集团	多方安全计算、联邦学习
21	XFL	2022 年 7 月	翼方健数	联邦学习
22	XSCE	2022 年 7 月	翼方健数	多方安全计算
23	mpc4j	2022 年 8 月	阿里巴巴	多方安全计算

五、发展热点问题分析

近年来，隐私计算技术快速发展，正在多行业逐步落地应用。在隐私计算应用阶段，应更加关注技术的安全特性如何在不同场景下保证合理应用，如何在保证安全的同时有效提升产品性能，差异部署的产品平台如何有效互联互通，实际应用中如何与相关法律法规的适配性等问题。因此本章将从技术本身特征出发，为适配不同场景应用进行隐私计算安全分级探讨，为大规模应用进行跨平台互联互通探讨，为持续健康发展进行合规性探讨。

（一） 隐私计算安全性分析

安全性是隐私计算的第一要素。隐私计算通过只输出中间参数、标签等信息，或在可信受控环境中对数据进行处理的方式，保障了数据的安全性，提高了数据流通的主动性。当前隐私计算的安全分级是技术在不同场景中应用过程中的重点、难点，隐私计算产品安全边界的界定需要考虑不同行业、不同场景和不同技术的差别，也需要平衡计算准确性和计算效率的要求。因此，安全风险点和安全分级思路亟需明确。

1.隐私计算安全性现状分析

隐私计算分支技术的安全根基各不相同，需要形成通用的评价方法来验证、度量隐私计算技术的安全性。隐私计算交叉融合了密码学、人工智能、计算机硬件等众多学科，形成了多方安全计算、联邦学习、可信执行环境等主要技术路线，各分支技术的安全根基各不相同。多方安全计算基于密码学，针对密态数据进行多方联合计算，在固定的安全模型下，能够达到可证明安全；联邦学习基于分布式机器学习、差分隐私等，计算过程中仅传递处理后的中间数据，保护了各方隐私数据的安全；可信执行环境依赖于硬件，通过隔离技术，为使用者创造了一个安全可信的执行空间，并提供了代码和数据的保密性和完整性保护。然而，在客观现实世界中，绝对安全的系统是不存在的，随着技术的不断发展，新的安全威胁也会持续产生。因此，对于隐私计算技术安全性的验证与度量至关重要。

除技术自身的安全性外，算法实现、密码模块、通信框架、节点系统等都会影响产品整体的安全性。虽然隐私计算的核心是计算，但是从技术应用和产品的角度，除了算法协议原理的安全性，还需综合考虑算法工程化实现、产品使用的密码模块和通信框架、调度管理功能的设计与实现等多方面的安全性，系统整体的安全性由其中最薄弱的环节来界定。

现实应用场景的安全需求不同，应结合场景需求对隐私计算产品进行安全分级。站在应用需求方的角度看，使用隐私计算是为了在保护隐私的前提下实现数据安全流通，发挥数据价值。然而，流通过程中的数据可控程度和价值损失程度两者之间难以兼顾。在实际应用中，

各场景对应的参与方信任程度不同、数据类型不同，这造成了其需要达到的数据可控程度也是不同的。一味的追求高安全水平可能会造成数据价值无法达到预期，导致各主体的参与积极性降低。分级框架的形成，有助于推动技术应用方结合其自身业务需求选择适当安全等级的方案，实现数据可控程度和数据流通价值的最大化。

2.隐私计算安全分级探索

近年来，业内逐步开始了对隐私计算产品安全分级的实践探索，在中国信通院“可信隐私计算”标准和评测体系中，首次提出了针对多方安全计算、联邦学习产品算法协议部分的安全分级，为行业供需双方提供了参考指导。在国际标准方面，IEEE P2986、P3169 等项目中也都开展了对隐私计算产品的安全分级的深入讨论。

针对隐私计算产品的安全分级，主要包括以下三个步骤:

一是全面梳理产品的潜在安全威胁。只有全面、系统地识别出威胁，才能有效地进行后续的风险评估与等级评定。当前应关注算法协议和平台产品的主要安全威胁主要包括节点系统、应用平台、通信网路、算法实现、数据与文件、密码安全、镜像安全、身份认证、流程制度等方面（见附录 3）。

二是定量分析产品的数据保护程度。根据各分支技术产品的威胁模型与环境模型（可能发生威胁的操作和技术），设置统一的数据保护程度评价指标。结合主动攻击和定量分析的评价方式，预测各威胁场景或单个威胁事件的可能性和影响程度，进而得到威胁的风险严重性以及产品所能达到的数据保护程度，做到安全可验证、可度量。

三是对产品的安全评测与等级评定。结合各行业的数据分类分级要求，确定各业务场景的安全基线。依据前序步骤得到的威胁列表、各威胁的风险严重性以及产品的数据保护程度，结合各实际业务场景的安全需求，实现场景化的隐私计算产品安全等级评定。

（二） 隐私计算性能分析

隐私计算能够实现如基础运算、联合统计、安全求交、隐匿查询和联合建模等多类应用，但由于算法实现中涉及大量的密码学操作和通信带宽等资源限制，当前隐私计算的性能仍有待提高，这也是阻碍隐私计算更大规模应用的主要因素之一。

1.隐私计算性能现状分析

目前，隐私计算算法在安全求交和联合建模等场景中的性能有待提升。隐私计算各类算法在不同条件和场景下耗时差异大，所以考量性能应使用固定的硬件资源和数据集，同时算法满足安全性和结果准确性的要求。其中，安全性指的是产品应保证数据在传输中的安全性、算法安全和密码的安全强度达标等，另外对于可信执行环境产品，应满足内部的计算环境安全性。准确性是指隐私计算产品所使用的某些特定算法可能会导致加密计算结果与明文存在一定程度的偏差，在实际应用中，小范围内的偏差是可接受的。

根据中国信通院发布的隐私计算性能标准和测试统计结果，基础运算和联合统计通常作为其他复杂运算的算子，计算性能普遍较高。在隐匿查询场景中，典型的实现方案有 XPIR，KeywordPIR 等，当前单次的百万级不可区分度的隐匿查询最快可达到秒级，隐匿查询在某

些场景已达到可用程度。对于安全求交，典型的方案包括基于 RSA 盲签名的方案，基于不经意传输扩展的方案等，不同方案由于计算量和通信量不同，所以有着不同的适用场景。例如，两数据方均持有一亿数据量的平衡场景的耗时在半小时左右，非平衡场景较平衡场景耗时少；三数据方场景的耗时有一定增加，平均耗时接近小时级。联合建模场景中，对于两方各持有几十万行乘以几千维度量级的数据集进行逻辑回归建模，使用基于秘密分享的方案和基于同态加密的联邦学习方案均接近一小时完成，但后者相比较快，而对于树模型建模，由于涉及运算更复杂，用典型的 SecureBoost 方案建模平均耗时在小时级以上，如果使用多方安全计算的方式则耗时更长，并且随着数据规模逐渐增大到百万级，建模的性能会更差。

2.隐私计算性能优化方法

性能提升可以从算法层面优化与硬件层面加速相结合实现。在算法层面，一是可以进行并行化处理，如数据并行处理、算法并行操作或工作流水线并行等，充分利用现有资源提升效率；二是针对于联邦学习模型，可通过模型压缩控制每轮信息传输大小和通过增加本地计算降低交互轮数的方式提高通信效率；三是在充分考虑场景的安全性和准确性的前提下，可通过使用差分隐私手段牺牲准确性来换取可能的性能提升。在硬件层面，当前也出现了专用的加速卡和隐私计算一体机产品，原理是将同态加密等复杂运算转移至 GPU、FPGA 和 ASIC 等硬件设备上执行，以硬件加速方式缩短计算耗时。

（三） 隐私计算互联互通分析

互联互通是构建基于隐私计算的数据流通基础设施的必经之路。当前隐私计算技术产品百花齐放，产品在算法协议、任务调度和管理等方面存在较大差异，为实现多方数据融合，用户往往要付出极高的沟通成本甚至重复建设系统平台。着眼广阔的数据要素流通前景，构建基于隐私计算的数据流通基础设施，以跨平台互联互通为前瞻目标，探索兼容性强、开放度高的互联互通协议，有望推动数据流通基础设施的建设落地。

1.隐私计算互联互通现状分析

隐私计算互联互通需要统一规范的接口、协议等实现跨平台的数据、算法、算力的交互与协同。从“底层通信—中间层交互—顶层应用”的角度出发，各个层次都需要不同程度的规范，需要隐私计算生态各方达成共识，才能合力走向最终互通。通信层要对平台间选择的通信框架、通信内容、通信安全、传输机制等内容进行规范。交互层要从节点、资源和算法执行三个维度进一步约定跨平台交互过程中在发布、认证、查询、授权、连接调用、信息和状态同步等环节的规范流程和要求。应用层则是在规范通信要求和互联协议的基础上统一计算任务实现过程中的协同管理，既包括任务编排、调度、执行、监控和存证等方面的统一规则，也包括不同类型计算任务的实现流程的协商约定。

隐私计算行业正在积极探索互联互通的可行方案，但由于技术原理的复杂性和产品形态的多样性，目前仍存在诸多困难。一是算法原

理和实现的差异性，隐私计算本身涉及算法众多，计算逻辑和数据交互流程难统一，算法的实现方案强依赖产品设计框架。二是系统设计过程和平台功能组件的多样性，完整的计算平台还包括授权认证、任务编排调度等控制管理功能，不同平台整体架构的研发思路和应用设计各异，协同完成同一计算任务需解决平台间兼容适配的问题。三是技术提供商改造驱动力不足，实现互联互通势必存在一定程度的妥协、损失原有产品的部分个性化，目前隐私计算的应用探索仍在推进,处在增量用户拓展阶段,在进入存量竞争之前,互联互通对于部分技术厂商而言并非“刚需”。

2.互联互通解决思路

首先，标准规范是实现互联互通的先决条件。比如互联网数据传输场景中 TCP/IP 协议、移动通信 3G、4G 等标准化协议、银联银行卡跨行交易的通用报文协议、国内外物联网的跨平台接入协议等都是通过制定系列标准化的协议,约定不同的设备如何组织和接入同一网络并进行数据交互。因此，互联互通应对平台间通信协议、互联协议和任务实现流程等基础环节提出标准化技术规范。以互联协议为例，以算法互联为例，在各方协商对齐节点、数据等资源的基础上，从调度层到算法层，基于“异构一层、规范一层”的思路，算法调度互联需要制定统一的调度接口规范，开放算法互联则需要一系列具体算法的开放协议规范。

同时，适配业务场景是验证互联互通方案的本质要求。互联互通不只是需要在技术层面进行攻关，统一标准，更需要在应用层面继续

突破。互联互通的目标是满足多方数据融合的应用需求，避免形成数据群岛，所以只有适配业务场景、解决业务现实问题的技术方案才是可推广可验证的方案，才是实现隐私计算技术规模落地应用的可行方案。

此外，由于隐私计算技术发展尚未成熟，要实现技术产品互联互通乃至形成互联生态都需要多方协作共同探索。不管是算法迁移还是算法对齐的互联方式，隐私计算技术厂商都需要进行一定程度的妥协，或是打破原有平台的自治性或是失去部分算法的独立性。但是，随着行业各方(技术提供方、技术应用方、标准化组织等)持续探索，互联互通最终将在尽量保持平台内部自治性、最大程度降低改造成本、减少对平台技术影响的基础上，允许技术平台动态地自由加入或退出互联互通网络，从而构建完善的生态网络，助力数据安全流通。

（四） 隐私计算合规性分析

《中华人民共和国个人信息保护法》（以下简称“《个人信息保护法》”）针对个人信息处理者规定了取得授权同意、进行个人信息保护影响评估等较为严格的合规要求。对于隐私计算技术能够在何种程度上帮助企业履行《个人信息保护法》规定的合规义务，目前仍需探讨。对此，我们认为，隐私计算技术本身并不能免除相关主体在《个人信息保护法》下应当履行的合规义务，但对于增强数据处理的安全性，降低数据滥用风险方面具有积极的意义。

1.隐私计算技术的合规价值现状分析

探讨一：使用隐私计算技术处理个人信息，是否还需要取得个人

授权同意？一些观点认为，在隐私计算技术处理个人信息的过程中，个人信息未出域，因此无须取得个人任何授权同意。但个人信息是否出域并非是判断是否应当取得个人同意的标准。除了《个人信息保护法》第十三条规定的例外情形，处理个人信息应当取得个人同意。因此，在不符合法定例外情形的情况下，当前使用隐私计算技术处理个人信息应当取得个人授权同意。

探讨二：个人信息经过隐私计算处理后是否达到了匿名化？隐私计算使用加密等方法对原始数据进行了保护，但仍有被恶意解密出相关信息的风险。根据《个人信息保护法》第七十三条：“……（三）去标识化，是指个人信息经过处理，使其在不借助额外信息的情况下无法识别特定自然人的过程。（四）匿名化，是指个人信息经过处理无法识别特定自然人且不能复原的过程。”因此，当前隐私计算并不能完全达到绝对匿名化。故个人信息经过隐私计算技术处理后，后续的处理相应的仍然要遵守《个人信息保护法》的相关合规要求。

探讨三：使用隐私计算技术是否可以满足目的限制要求？在某些场景下，隐私计算技术的应用可以满足《个人信息保护法》第六条规定的“**收集个人信息应当限于实现处理目的的最小范围**”。但隐私计算处理的密文、随机分片、梯度等是否满足“处理个人信息应当与处理目的直接相关并采取对个人权益影响最小的方式”，并无法仅仅通过隐私计算技术本身来解决。满足目的限制的要求还需要各参与方使用隐私计算技术并结合授权情况、应用场景等限定使用目的，以满足合规要求。

2.隐私计算技术的合规优势

隐私计算技术的合规优势在于增强数据处理的安全性。保障数据安全是数据合规的重要组成部分，这在《中华人民共和国数据安全法》和《个人信息保护法》中均有体现。隐私计算技术诞生之初就是为了降低数据在使用和流通过程中的安全风险，在原始数据不被其他方知悉的情况下，也能够对其进行开发利用，同时降低数据滥用的可能性。从增强数据处理的安全性看，隐私计算技术具有很高的合规价值。但**如何能够将隐私计算的合规价值最大化，还取决于如何应用。**隐私计算技术并非是帮助履行《个人信息保护法》合规义务的专用技术工具。企业在落实《个人信息保护法》合规义务的过程中遇到的问题并非隐私计算技术原本试图解决或擅长解决的问题，而是需要未来立法、监管、理论研究和行业实践共同探索和解决的。因此，仅仅将隐私计算技术用于解决授权、匿名化等合规问题，可能无法达到预期的效果；相反，如果将应用的重点放在更好的解决数据处理的安全性问题，隐私计算技术的合规价值将更加凸显。

隐私计算技术可以降低数据泄露和数据滥用风险。比如，商业银行针对客户的贷款行为进行风控时，往往需要丰富的数据对客户进行更精准的画像，但数据一旦对外共享，可控性将大大降低，通常也只能通过追究违约责任的方式对数据泄露和滥用行为进行事后补救，因此银行不愿、不敢与同业共享数据，导致金融监管机构无法有效对金融业务风险进行综合动态监测与预警研判。而隐私计算技术结合隐匿求交、逻辑回归或树模型等联合建模及预测等技术，可以做到“数据

不出域”、“数据不动、模型动”。一方面，参与交互的数据减少，从源头上降低了数据泄露的风险；另一方面，数据共享过程中合作方无法获取原始数据，也就无法超出授权范围对原始数据进行使用，从而降低了数据滥用风险。

为了发挥隐私计算技术增强数据处理安全性方面的合规优势，首先应当**保证隐私计算技术本身的技术、安全和性能等各方面能够达到相关标准，并根据应用场景选择合适的技术类型。**目前针对基于多方安全计算、联邦学习、可信执行环境的数据流通产品或平台的技术要求、安全要求、产品性能要求和测试方法，以及隐私计算跨平台互联互通、隐私计算面向金融场景的应用规范等，都已有相关标准出台，可作为参考依据。此外，由于隐私计算技术本身涉及多方参与，**在提供数据、进行计算、输出结果等环节中涉及的各参与方合规义务等也应当予以重视。**

六、总结与展望

随着我国数字经济持续纵深发展，数据已成为数字经济基础性要素，而数据的安全高效可信可控流动变得尤其重要，隐私计算作为数据流通的重要创新前沿技术，正处于产业快速增长阶段，应用场景进一步丰富，基于金融、政务、医疗、互联网等数据密集型行业已开展落地实践，提升我国传统场景的应用安全并满足了新兴场景的应用需求，覆盖金融风控、精准营销、政务服务、医疗健康等。

从技术层面来看，实现多技术的融合将成为未来技术的一大趋势。当前多方安全计算、联邦学习、可信执行环境仍然是隐私计算的三大

主流技术方向，不同技术之间核心技术有所侧重，但都面临单一技术的瓶颈限制，而多技术的融合可以突破隐私计算单类技术瓶颈。同时，软硬件技术的协同发展，也将大大提升产品可用性，推进隐私计算技术进一步向前迈进。

从应用层面来看，隐私计算的落地正在由传统场景延展到新兴场景中。相较于传统的数据流通应用模式，隐私计算能够更加有效的保护各个合作方的数据安全，且可以具备数据价值计量功能。由于技术路线的多样性，在应用中不同技术路径之间的差异明显，而同一路径下不同产品的实现方案也相互独立，跨技术路径、跨系统平台之间的隐私计算的互联互通将成为亟需解决的问题。

从行业层面来看，隐私计算经历了萌芽期的理论完善、探索期的技术创新，已经进入到行业的快速增长阶段。伴随强烈的市场需求，隐私计算已成为商业和资本的热门赛道，并逐渐形成由供需双方共建的健康行业生态。当前发展阶段下，隐私计算行业既充满机遇又面临挑战。一方面，随着竞争者数量增加以及产品数量增多，行业竞争策略发生改变，部分企业可能会迎来新的挑战；另一方面，只有产品的技术能力和应用模式越发成熟之时，隐私计算才有望成为全社会数据流通的基础设施。

随着产业政策、示范项目、政产学研的引导，以隐私计算为代表的一类数据安全流通技术正在成为筑牢数字安全屏障、促进数字经济持续健康安全发展的基础设施。未来，隐私计算产业发展仍需要坚持“安全和可信”的核心原则，凝聚行业应用需求方、隐私计算技术提

供方、硬件支持方三类主体力量持续推动隐私计算核心技术创新和落地落实，促进数据要素的可信安全流通。

附录

附录 1 隐私计算存量优化应用场景典型案例

编号	案例名称	参与方	数据类别及规模	技术采用	应用效果
1	基于隐私计算的联合建模营销应用	金融机构、大数据科技企业	行为轨迹、兴趣偏好	联合分析、联邦学习、区块链	能较好地在沉默用户中筛选出具有金融产品需求的优质客户，帮助金融机构实现存量客户高效触达、提升用户转化率。
2	基于隐私计算的政银联合风控系统	金融机构、政府部门	亿级客户 ID、百维特征：企业经营、金融数据	联邦学习	为金融机构在贷前大幅提高授信效率；在贷中降低信息不对称性与不透明；在贷后挖掘出潜在高风险企业，提升监测能力。
3	基于隐私计算的汽车保险业务应用	金融机构、汽车企业、大数据科技企业	汽车属性、保险数据	联邦学习	减少保险公司因信息盲区导致的骗保事件，降低赔付成本。
4	基于隐私计算的风险信息协同共享平台	金融机构	亿级客户 ID：风险数据	隐私求交	在金融机构间实现风险黑灰名单库共享，搭建金融同业联盟。
5	基于隐私计算的智能出行风控系统	互联网企业、通信运营商	十万级客户 ID、500 维特征：行为轨迹、通信数据	联邦学习	解决了出行平台上新用户不能风控预测的问题，实现了对坏账比例的有效控制。
5	基于隐私计算的联合营销及客户运营优化	金融机构、运营商、互联网企业	亿级客户 ID、千维特征：金融数据、行为轨迹、兴趣偏好、电商消费、通信数据	隐私求交、联邦学习	增强金融机构在新开户阶段判断客户资质的能力，提升在存客提升阶段的精准识别和精准营销能力，通过千人千面的客户关怀方案设计提升用户满意度与客户粘性。
6	基于隐私计算的数据服务平台	金融机构、大数据科技企业、互联网企业	亿级客户 ID、千维特征：金融数据、行为轨迹、兴趣偏好	联合统计分析、联邦学习	挖掘目标用户，并对用户意向进行精准触达，节约推广成本的同时，有效提升了广告转化率，摆脱传统广告投放模式的高成本束缚。

编号	案例名称	参与方	数据类别及规模	技术采用	应用效果
7	基于联邦学习的存客运营分析系统	金融机构、大数据科技企业、互联网企业	50 万客户 ID: 金融数据、电商数据、风险数据	联合统计分析、联邦学习	为银行针对不同的用户类型提供多种可行的营销方案，同时在向用户精准营销时，也可以达到促活的目的，通过本方案降低金融机构的运营成本，提高收益金额。
8	数据要素安全流通案例	金融机构、互联网企业	金融数据、电商数据	隐私求交、联邦学习	帮助金融机构确认关联的客户群，在保证原始数据在物理和逻辑层面均不出域的前提下，为金融机构侧实现了精准的人群策略设计。
9	传染病多点触发监测和智能预警平台	政府、实体企业、大数据科技企业	医疗数据、网络搜索、地理位置、人员流动、政务数据	联邦学习	构建涵盖人员、物品及产品、环境及场所的全面智慧化预警多点触发机制，完善传染病疫情监测系统，织密不明原因疾病、聚集性病例和异常健康事件的监测网。
10	基于隐私计算的疫情以及传染病防控	医疗企业、医院、政府、实体企业、互联网企业、大数据科技企业	医疗数据、药物售卖、疫情数据	联合统计分析、区块链	通过隐私计算构建有效的新发和突发传染病预警系统，在第一时间发现潜在的传染病风险，并提供数据溯源等相关服务，做到传染病疫情的早发现、早报告、早处置，提高疫情实时分析、集中研判的能力。
11	基于隐私计算的药物临床试验与新药研发	医疗企业、医院	医疗数据、随访数据	联邦学习	利用隐私计算技术，打破数据孤岛，联合多中心多维度数据源，高效利用数据的同时保证患者个人隐私数据安全。
12	疾控中心赋能境外高校科研	医院、高校	医疗数据、科研数据	联邦学习	国外高校对科学研究成果进行发布，需要使用疾控中心的大量数据进行分析为理论成果作为支撑，基于隐私计算实现该数据数据流通过程需要可管、可控、可溯。
13	公安赋能教育局案例	政府	政务数据	隐私求交	公安人员将人口相关信息加密上传至隐私计算平台，在学生报名的时候，用户将用户基本信息加密提供给隐私计算平台，隐私计算平台根据政务数据与任务计算出结果，将结果数据（孩子是否满足报名要求）返回给用户。
14	大数据交易中心数据质押场景	金融机构、实体企业	金融数据、质押数据	隐私求交	保障企业的核心数据的安全，保证在抵押过程中的隐私，同时保障银行对数据的预授权，保证在无能力还款时，银行能获取正确数据以减

编号	案例名称	参与方	数据类别及规模	技术采用	应用效果
					小损失，最大化资金的使用效能
15	水电联合群租房治理案例	政府、大数据科技企业	政务数据	联邦学习	准确的识别结果显著减少政府部门走访、核查及整治群租现象所花费的人力物力和财力，并有效避免了大量因群租所导致的火灾等后果造成的严重财产损失。

附录 2 隐私计算增量创新应用场景典型案例

编号	案例名称	参与方	数据类别及规模	技术采用	应用效果
1	全匿踪联邦学习反电信欺诈案例	金融机构、运营商	电诈风险名单数据、银行开卡用户数据	全匿踪安全求交、全匿踪联邦学习、匿踪查询	突破了无需安全求交、不泄露交集ID、在全匿名数据集下进行联邦学习的技术难题，实现了交易反电信诈骗全流程安全合规，在保护转账人和转账信息安全的前提下，及时识别电诈转账风险，阻止电诈异常交易。
2	基于隐私计算的电信欺诈风险识别	金融机构、运营商、政府机构、互联网	风险特征数据、风险标签数据	隐匿查询、联邦学习	在安全合规的前提下，将敏感数据源安全融合，实现信息共享，达到区域联控效果，提升电信欺诈风险识别准确率和覆盖率，模型命中率相较于传统反欺诈风控模型有显著提高。
3	基于隐私计算的用户三要素核验	金融机构、运营商	用户基础信息	隐匿查询、隐私求交	基于隐私计算的实现用户三要素核验，能够在安全合规的前提下完成金融机构对用户和业务审核的风控识别。
4	基于隐私计算的智能风控管理平台	金融机构、征信机构、运营商	金融贷款用户数据、征信风险名单、银行卡支付数据、电商平台用户的交易数据	隐匿查询、联邦学习	在保护用户信息不泄露的前提下，构建更精准大数据风控模型，从贷前、贷中、贷后查询或测算借款自然人的表现。
5	基于隐私计算的多方联邦广告营销系统	广告主机构、流量平台机构、数据提供方	用户平台使用习惯数据、用户消费习惯数据	隐匿查询、联邦学习	运用有限的 CRM 数据进行联邦学习训练的精准模型，在较短的广告营销活动周期中，也获得了高质量曝光。

附录 3 隐私计算产品安全威胁识别清单

维度	威胁点
节点系统	允许或被绕过授权修改 TCB 范围内的代码；攻击操作系统访问隔离的程序；侧信道攻击导致泄露密钥信息；分支预测攻击；微体系采样攻击等。
应用平台	节点运行程序一致性和硬件环境合法性未做远程认证；异构平台系统之间未做远程验证；平台提供“由用户控制”的命令/代码执行功能；以某参与方身份向另一节点下发恶意指令；应用前端输入中没有对不可信入参做安全过滤；利用供应链应用漏洞，如三方包、三方软件等；利用应用平台架构设计或开发实现的漏洞；对外发布的 SDK 包含内部敏感信息；容器内执行恶意命令导致横向渗透并获取敏感信息；关键环节或代码未进行形式化验证；发版前缺少安全攻防实战验证等。
通信网络	节点间通信数据泄漏或被篡改；敏感数据未进行二次加密处理；安全通信通道建立的过程与设计描述不一致；通信通道建立时未进行身份认证；RPC 通信未对反序列化类型进行校验；会话凭证可猜测/伪造或会话凭证失效等。
算法实现	未对算法逻辑安全进行检测验证；未对算法签发者一致性验证；未对参与方执行的计算任务进行一致性验证；利用算法设计或代码实现的漏洞等。
数据和文件	重要数据或敏感数据未加密存储；数据存储时认证口令无保护；隔离的任务数据被其他任务获取使用；计算任务中封存的密文数据被非法解密；参与方计算结果未加密或非认证使用方也可以解密；参与方计算结果被篡改；未对参与计算任务的数据进行一致性验证，或未对数据使用方进行合法性验证；后端返回程序开发信息、应用配置信息、隐私信息或服务器信息导致敏感信息泄漏；数据在使用完毕之后无销毁；参与方对数据使用中的关键环节未进行存证；不支持快速检索出计算异常和追溯错误原因等。
密码安全	密钥体系设计和实施不合理；密码算法实现不正确；生成随机数不具有随机性等；弱签名算法或算法使用不当导致不安全的签名算法等。
镜像安全	镜像使用的系统有严重/高危漏洞状态；镜像使用的三方组件有严重/高危漏洞；镜像中应用系统存在空口令/弱口令/默认口令；推送的镜像含敏感信息；对镜像仓库里镜像进行投毒等。
日志	参与方未采用日志对平台系统、数据库访问及操作记录；业务日志未加密存储；敏感信息未脱敏打印；日志内容没有限制访问权限等。
身份认证	认证机制失效导致非法身份获得认证；认证凭证泄漏；不正确的认证协议设计或实现导致逻辑绕过等。
流程制度	缺少发版或云上线的流程要求；缺少产品安全管理规范和实施要求等。

参考文献

[1] 国务院办公厅. 要素市场化配置综合改革试点总体方案[EB/OL]. 2021. http://www.gov.cn/zhengce/content/2022-01/06/content_5666681.htm.

[2] 国务院. “十四五”数字经济发展规划[EB/OL]. 2021. http://www.gov.cn/zhengce/content/2022-01/12/content_5667817.htm.

[3] 中共中央，国务院. 关于加快建设全国统一大市场的意见[EB/OL]. 2022. http://www.gov.cn/gongbao/content/2022/content_5687499.htm.

[4] 中国隐私计算产业发展报告（2020-2021），国家工业信息安全发展研究中心，2021.

[5] 《Gartner 2022 隐私技术成熟度曲线》，Gartner，2022.

[6] Shamir A. How to share a secret[J]. Communications of the ACM, 1979, 22(11): 612-613.

[7] Blakley G R. Safeguarding cryptographic keys[C]//Managing Requirements Knowledge, International Workshop on. IEEE Computer Society, 1979: 313-313.

[8] 隐私计算联盟，中国信通院云大所. 隐私计算白皮书（2021 年）[R]. 2021.

[9] Yao A C. Protocols for secure computations[C]//23rd annual symposium on foundations of computer science (sfcs 1982). IEEE, 1982: 160-164.

[10] Yao A C C. How to generate and exchange secrets[C]//27th Annual Symposium on Foundations of Computer Science (sfcs 1986). IEEE, 1986: 162-167.

[11] ARM. ARM Security Technology-Building a Secure System using TrustZone Technology. ARM Technical White Paper, 2009.

[12] 闫树, 袁博, 吕艾临等.《隐私计算——推进数据”可用不可见”的关键技术》[M]. 电子工业出版社,2022-03-01.

[13] 魏凯，闫树，吕艾临. 数据要素市场化进展综述[J]. 信息通信技术与政策，2022(08): 59-64.

[14] Gentry C. Fully homomorphic encryption using ideal lattices[C]//Proceedings of the forty-first annual ACM symposium on Theory of computing. 2009: 169-178.

[15] Anati I, Gueron S, Johnson S, et al. Innovative technology for CPU based attestation and sealing[C]//Proceedings of the 2nd international workshop on

hardware and architectural support for security and privacy. New York, NY, USA: ACM, 2013, 13(7).

[16] McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Artificial intelligence and statistics. PMLR, 2017: 1273-1282.

[17] Yang Q, Liu Y, Chen T, et al. Federated machine learning: Concept and applications[J]. ACM Transactions on Intelligent Systems and Technology (TIST), 2019, 10(2): 1-19.

[18] Dash B, Sharma P, Ali A. Federated Learning for Privacy-Preserving: A Review of PII Data Analysis in Fintech[J]. International Journal of Software Engineering & Applications, 2022, 13(4): 1-13.

[19] Gentry C. A fully homomorphic encryption scheme[M]. Stanford university, 2009.

[20] 贾轩, 白玉真, 马智华. 隐私计算应用场景综述[J]. 信息通信技术与政策, 2022,48(5):45-52.

[21] 闫树, 吕艾临. 隐私计算发展综述[J]. 信息通信技术与政策, 2021, 47(6): 1.

[22] Liu J, Jin W, He Z, et al. HUT: Enabling High-UTility, Batched Queries under Differential Privacy Protection for Internet-of-Vehicles[J]. arXiv preprint arXiv:2202.06495, 2022.

[23] Yue D, Chengqi Y, Qianqian H, et al. Constructing a Common Data Circulation Infrastructure Platform for the National Unified Data Factor Market——Technical Path and Policy Thinking of Constructing the National "Data Networking" Root Service System[J]. Data Analysis and Knowledge Discovery, 2022, 6(1): 2-12.

[24] Huang Z, Lu W, Hong C, et al. Cheetah: Lean and Fast Secure Two-Party Deep Neural Network Inference[J]. IACR Cryptol. ePrint Arch., 2022, 2022: 207.

[25] Watson J L, Wagh S, Popa R A. Piranha: A GPU Platform for Secure Computation[C]//31st USENIX Security Symposium (USENIX Security 22). 2022: 827-844.

[26] Badrinarayanan S, Das S, Garimella G, et al. Secret-Shared Joins with Multiplicity from Aggregation Trees[C]//Proceedings of the 2022 ACM SIGSAC

Conference on Computer and Communications Security. 2022: 209-222.

[27] Garimella G, Rosulek M, Singh J. Structure-Aware Private Set Intersection, With Applications to Fuzzy Matching[C]//Annual International Cryptology Conference. Springer, Cham, 2022: 323-352.

[28] Zhang X, Gu H, Fan L, et al. No free lunch theorem for security and utility in federated learning[J]. arXiv preprint arXiv:2203.05816, 2022.

[29] Liu Y, Kang Y, Zou T, et al. Vertical Federated Learning[J]. arXiv preprint arXiv:2211.12814, 2022.

[30] Liu Y, Zhang X, Kang Y, et al. Fedbcd: A communication-efficient collaborative learning framework for distributed features[J]. IEEE Transactions on Signal Processing, 2022, 70: 4277-4290.

[31] D. Cai, T. Fan, Y. Kang, et al. Accelerating vertical federated learning[J]. IEEE Transactions on Big Data, 2022.

[32] Wu Z, Li Q, He B. Practical Vertical Federated Learning with Unsupervised Representation Learning[J]. IEEE Transactions on Big Data, 2022.

[33] Khan A, ten Thij M, Wilbik A. Communication-Efficient Vertical Federated Learning[J]. Algorithms, 2022, 15(8): 273.

[34] Chen W, Ma G, Fan T, et al. SecureBoost+: A High Performance Gradient Boosting Tree Framework for Large Scale Vertical Federated Learning[J]. arXiv preprint arXiv:2110.10927, 2021.

[35] Jia Y, Liu S, Wang W, et al. HyperEnclave: An Open and Cross-platform Trusted Execution Environment[C]//2022 USENIX Annual Technical Conference (USENIX ATC 22). 2022.

联系方式：

隐私计算联盟

地址：北京市海淀区花园北路 52 号

邮编：100191

邮箱：jiaxuan@caict.ac.cn

网址：www.caict.ac.cn