数据要素研究系列
编号：DE-2021-02

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 年 5 月

报告编写组

参编单位：

国家工业信息安全发展研究中心

中国电子商会数据资源服务创新专业委员会

蚂蚁科技集团股份有限公司

翼健（上海）信息科技有限公司

华控清交信息科技（北京）有限公司

参编人员：

孙　璐	杨　玫	杨　捷	乔思渊	刘　巍
李　玮	周易江	杨　柳	骆伊宁	冯立鹦
毛庆凯	卢　龙	闫守孟	张本宇	樊振华
陈超超	杜　健	袁鹏程	王　力	李克鹏
薛　峰	段　普	王　磊	韦　韬	冯　超
邵　青	纪润博	张霖涛	张莺耀	

版权声明

前　言

2020 年 4 月，《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》发布，将数据作为一种新型生产要素，与土地、劳动力、资本、技术等传统要素并列。2020 年 10 月，《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》要发布，其中提出加快建设数字经济、数字社会、数字政府，建设数字中国，打造数字经济新优势，明确数据作为核心生产要素的重要性。

数据成为生产要素并促进数字经济高质量发展，前提是要充分发挥数据这一新型要素对其他要素效率的倍增作用，培育发展数据要素市场，使大数据成为推动经济高质量发展的新动能。但是，当前在数据要素价值盘活过程的数据生产加工、数据资源汇聚、数据流通交易、数据模型训练与部署过程中仍然面临数据确权难、投入成本高、数据集质量低、数据资源有限等问题。在此背景下，在政策驱动、市场需求同时作用下，催生出数据流通共享技术新赛道——隐私计算。宏观层面，隐私计算将成为新一代信息技术领域基础性、支撑性环节，很大程度上完善了各类软件应用及平台安全性、合规性，促进了大数据、人工智能产业的健康、可持续、高质量发展。微观层面，隐私计算使企业在数据合规要求前提下，充分调动数据资源拥有方、使用方、运营方、监管方各方主体积极性，实现数据资源海量汇聚、交易和流通，进一步盘活了第三方机构数据资源价值，促进数据要素的市场化配置。

在本报告撰写过程中，国家工业信息安全发展研究中心通过专家访谈、企业调研、案头研究等方式开展隐私计算相关研究，得到众多相关企业的配合与支持。报告内容从背景、技术、产业等维度出发，阐述了我国隐私计算的发展现状，并基于现阶段面临的问题提出政策建议。

由于编者水平有限，本报告难免存在疏漏与不足，恳请各界同仁阅后批评指正，加强合作交流。

报告编写组

二〇二一年五月

目　录

图 目 录

表 目 录

第一章 背景篇

隐私计算本质上是在保护数据隐私的前提下，解决数据流通、数据应用等数据服务问题。基于以上特性，隐私计算在个人隐私权、企业数据权益、社会发展平衡保障下释放数据要素价值，成为与法律、监管强相关的技术，且能够支持对企业的数据资产权益（定价权、控制权）的保障。

一、基本概念

隐私计算作为技术体系，概念诞生时间较短，但多方安全计算、联邦学习、可信执行环境等作为隐私计算的重要技术分支，理论基础的研究已开展多年。隐私计算概念的确定有助于技术体系的完善及各技术间的融合发展。

（一）国内隐私计算定义

隐私计算是指在提供隐私保护的前提下实现数据价值挖掘的技术体系，而非单一技术，早期多被定义为隐私保护计算、隐私保护技术等。2016 年发布的《隐私计算研究范畴及发展趋势》正式提出“隐私计算”一词，并将隐私计算定义为“面向隐私信息全生命周期保护的计算理论和方法，是隐私信息的所有权、管理权和使用权分离时隐私度量、隐私泄漏代价、隐私保护与隐私分析复杂性的可计算模型与公理化系统。”

随着数字技术的发展，隐私计算内涵、特征及代表技术不断演进。主流技术研究焦点从 2016 年的数据扰乱、数据匿名化进展

至今日的包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系，涵盖同态加密、多方安全计算、差分隐私等众多技术方法。现阶段，隐私计算指带有隐私机密保护的计算系统与技术（硬件或软件解决方案），能够在不泄露原始数据前提下，对数据进行采集加工分析处理分析验证，包括数据的生产、存储、计算、应用等数据处理流程的全过程，强调能够在保证数据所有者权益、保护用户隐私和商业秘密的同时，充分挖掘发挥数据价值。

（二）国外隐私计算概念

国外隐私计算被定义为“Privacy Enhancing Technologies”（PETs），即隐私增强技术。2001 年，隐私增强技术概念提出，即“一套信息和通信技术措施系统，在保障系统功能的前提下，通过消除或减少个人数据或防止对个人数据进行不必要和/或不希望的处理来保护隐私。”具体而言，隐私增强技术广义上指保护个人或敏感信息隐私性的任何技术方法，包括例如广告拦截、浏览器扩展插件等相对的简单技术。狭义上，隐私增强技术主要指互联网信息所依赖的加密基础结构，即联邦学习、多方安全计算、零知识证明等“新兴”隐私增强技术。

出于对隐私保护的重视，国外在该领域的研究受到国家及国际组织层面的重视，定义中强调隐私增强技术作为数据保护规则的作用意义。例如，世界经合组织 2002 年的报告中指出隐私增强技术是有助于保护个人隐私的广泛技术，从提供匿名性的工具到允许用户选择是否、何时以及在何种情况下披露个人信息的工具。

此外，美国通过法案将隐私增强技术定义为“任何软件解决方案、技术流程或其他技术手段，用以增强数据的隐私和机密性”，特别包括“匿名化和假名化技术、过滤工具、反跟踪技术、差异隐私工具、合成数据和多方安全计算”。

（三）数据流通模式差异性

传统数据服务以数据包形式（1.0）和明文数据 API 接口（2.0）进行流通与应用。1.0 模式典型方式是通过数据交易平台就数据所有权进行交易，但由于数据确权相关法律法规不明晰，该模式有较高的数据安全风险，较难保护数据所有者利益，易导致涉及用户隐私的信息暴露以及数据被使用方二次利用甚至滥用，因此近些年来该模式增长开始逐渐放缓。2.0 模式将加工处理完的单方结果数据以 API 形式输出，具体通过程序对元数据进行隔离，在用户发出数据使用请求后，由程序从元数据中抽取、调用数据反馈给用户。该模式下按照数据分类沉淀的 API 接口日调用量可达到上亿次，满足较广的服务覆盖范围，且一定程度保护了用户隐私信息以及降低二次利用可能性，但同时降低了数据价值融合的可行性。隐私计算有望发展成为数据服务 3.0 模式，直接作用于数据使用方面，能够通过协议或算法使得数据计算服务在不泄漏原始数据的前提下充分挖掘数据价值。

二、作用意义

近年来，新一代信息技术大部分是聚焦于信息化方式方法，如数据库、操作系统、网络通信、云计算、大数据等，保障系统畅通运行与业务稳定开展的相关数字技术业已成熟。隐私计算聚

焦数据共享开放领域应用，解决现阶段数据保护与数据流通多方面痛点，在政策驱动与市场需求双重作用下发展迅速。

（一）隐私计算助力数据要素市场化配置

随着技术手段创新发展、数字化转型步伐加快，数据已经变成了重要的增长点，获得维度更广、质量更优、层次更深的数据对于任何一个市场主体来说都变得十分重要。2020 年,《中共中央、国务院关于构建更加完善的要素市场化配置体制机制的意见》正式发布，首次将数据与土地、劳动力、资本、技术等传统要素相并列，指出了五个要素领域的改革方向，明确了完善要素市场化配置的具体措施。但数据使用面临的诸多问题尚未解决，如数据的要素化应用过程中如何确定数据归属权、如何保障数据隐私安全、如何确定数据使用权责、如何防止数据价值稀释等。传统的技术与手段无法有效解决上述问题，数据要素的合理化利用需要合法合规技术与业务创新模式的有力支撑。

培育数据要素市场的根本是数据资产化。只有保障数据资源的价值、解决数据权属关系边界模糊的问题，才能使数据具备权利属性进而设定为资产。一方面，隐私计算可保障数据的商品价值、交换价值及使用价值。传统模式下，数据复制性强的特点使原始数据转化过程中价值稀释显著，导致使用率越高价值越低。隐私计算在不交换原数据的前提下输出数据蕴含的知识，数据使用率越高证明数据应用价值越高，因此隐私计算是还原数据资产特性的根本，可以使数据资产价值以市场化的方式计量，有望成为数据资产化系统性工程中的重要环节。另一方面，隐私计算可

保障数据资产权属利益。按照资产属性，数权具有私权属性和公权属性。维护个人利益是私权属性的根本体现，公权属性则强调数据作为公共产品的资源性，主要指国家机关等公共部门出于公共利益目的而使用数据。隐私计算可有效平衡数据的私权属性与公权属性，不需要让渡数据个人权利即可使公共部门行使权力，有效消除数据壁垒，最大化释放数据价值。

（二）隐私计算成为防范数据泄露突破口

随着云计算、物联网与大数据等技术的不断发展，信息系统服务中针对用户数据的收集整理、分析预测手段不断成熟。各种定向服务基于位置跟踪、行为偏好记录，为人们日常生活提供诸多便利的同时，也越来越多地引发了隐私问题的关注。一方面，数据作为企业重要资产被深度开发利用。另一方面，数据构成公民个人生活的方方面面，各项在线服务过程中产生的海量数据不可避免地面临隐私泄露问题。近几年，大规模数据泄露事件频繁发生且呈现爆发递增趋势。根据安全情报供应商 Risk Based Security（RBS）的数据显示，2012 年至 2020 年数据泄露事件数量与涉及的数据量均在整体上呈现逐年递增趋势。国内数据泄露形势更加严峻：一是上亿级大规模重大泄露事件频频发生；二是涉及大量身份证号码、电话号码等个人基本信息以及人脸图像等生物识别敏感信息；三是数据泄露事件覆盖银行、快递企业、高校、互联网公司等各类机构主体。

数据泄露事件屡禁不止，使公众对于个人信息保护意识、敏感程度与认知水平全面提高，进一步给企业带来全新挑战。企业

若对原数据进行分析挖掘，获得公众完全的信任需对如何使用客户数据保持高度透明性，并在各项业务中以客户可信赖的方式执行，此外须提供完整的证据证明企业始终贯彻上述方针。但服务器暴露、安全性配置、员工监管等各环节都将导致企业对数据保护措施不力，完成以上三点要求成本压力过大。隐私计算尽管不能完全解决数据泄露问题，但基于密码学算法、去中心化、作用于数据交换过程等特点为隐私保护提供了新的解决方案。

（三）隐私计算促进多方数据安全合规协作

近年来，不断曝光的隐私数据泄露引起了监管部门的高度重视，数据安全、隐私保护相关的监管政策密集出台。我国已有《民法总则》《消费者权益保护法》《电子商务法》和《全国人民代表大会常务委员会关于加强网络信息保护的决定》《数据安全管理办法》等近 40 部法律、30 余部法规和 200 部规章制度，都涉及各类数据的保护条款，规定了企业对保护数据所负的法律义务。尽管目前法律体系相对分散、缺乏实施细则，但随着《个人信息保护法》《中华人民共和国数据安全法（草案）》《个人金融信息（数据）保护试行办法》等法律法规的研究制定，我国数据保护法律法规体系将更为清晰、严谨。2020 年 7 月，《深圳经济特区数据条例（征求意见稿）》发布，《条例》运用特区立法权率先展开地方数据立法，首提数据权，促进个人隐私保护。

数据立法及隐私保护机制的多方尝试，将使数据泄露维权困难、维权程序复杂、耗时过长、成本过高的情况进一步改善。在强监管趋势下，粗放型数据交易模式上升为触犯法律红线的行为，

目前业务仍处于此类灰色地带的企业将遭受重创，须积极探索符合合规要求的业务路线。隐私计算目前处于起步阶段，可以预见，随着国家对隐私数据监管的加强，企业对数据价值重视程度的提高，隐私计算将在2020-2030年实现爆炸式增长，有望发展成为数据共享基础设施的重要环节。

（四）隐私计算促进大数据进入新发展阶段

大数据产业是以数据生产、采集、存储、加工、分析、服务为主的相关经济活动，产业发展至今技术成熟、生态体系完善，借助大数据技术展现出的优势愈发显著，促使企业不断探索更高效的新技术对数据进行处理，包括数据的存储、查询和分析等。但大数据技术特点也带来以下问题：一是监督工作复杂、稽核难度大。大数据技术可广泛采集不同来源的数据，使传感器、社交网络等数据跟踪和状态控制难度加大。二是数据复用性强。数据蕴藏巨大商业价值，但扩散性强。当前数据产权意识有待提高，无法实行“谁采集、谁投入、谁受益”。三是数据推断与重新识别可能性提高。不同来源的数据集交叉合并分析，获得更多信息的同时也增加了隐私泄露风险。

数据价值的构成不在于数据本身，而是推动多种计算方式及应用，因此多方数据合作是大数据发挥价值的重点。但大数据难控制、复用性强、重新识别可能性高的问题限制了数据流通，一方面致使政务、医疗等敏感数据的分析挖掘受限，另一方面大数据技术及应用创新主体向掌握大量数据的互联网龙头企业倾斜，中小科技企业发展壁垒较大。隐私计算能够解决数据开放共享和

隐私安全保护的矛盾，可在保证原始数据安全隐私性的同时，实现对数据的计算和分析，有望成为打破大数据现阶段发展瓶颈的推动力。

三、国外政策环境

在现阶段数据驱动型创新应用蓬勃发展的关键时期，数据作为重要的基础战略资源，受到各国高度重视，欧美等发达经济体一方面在跨区域对外协定中强势约束数据流通相关条款，另一方面兴起对技术性隐私保护方法的理论研究及政策探索。

（一）欧盟发布技术指南肯定隐私计算的作用及价值

2020 年 7 月，欧盟法院（CJEU）在 Schrems II 中判定欧盟-美国隐私保护盾无效，美国不再根据欧盟通用数据保护条例（GDPR）第 45 条获得授权，可以在法律对等的基础上接收来自主要机制区域（EEA）的数据流。这意味着包括 Google、Amazon、Facebook 和 Microsoft 在内的 5300 多家美国企业失去了与欧洲经济共同体进行国际数据传输的权利。GDPR 合规门槛的提高，使企业更难获得和处理欧盟数据。欧盟-美国隐私保护盾的无效导致从欧洲经济区进行有效数据跨境转移必须依赖技术措施。欧盟法院（CJEU）和欧盟负责监督通用数据保护条例（GDPR）执行的欧盟数据保护委员会（EDPB）都强调，仅合同工具可能不足以保障在欧盟和美国之间按照 GDPR 要求传输数据。为寻求合规与发展的平衡，EDPB 发布“关于补充传输工具以确保符合欧盟个人数据保护水平的措施的建议 01/2020”，并于 2020 年 11 月通过，其中提出关于“拆分或多方处理”的建议，采用隐私增强技术成为欧

盟数据出口机构的尽职调查中，证明机构符合“采取必要的补充措施，对所传输数据的保护水平达到欧盟的基本等同标准”要求的证据。

在此背景下，2021 年 1 月 28 日，欧盟网络安全局（ENISA）发布《数据保护和隐私中网络安全措施的技术分析》，该技术指南将多方安全计算确定为适用于复杂数据共享方案的高级技术解决方案，尤其适用于医疗保健和网络安全领域。ENISA 在指南中建议各机构进行常规的“安全和数据保护风险评估”，以确定是否需要通过加密隐私增强协议降低数据处理中的风险。ENISA 是欧盟负责协调“整个欧洲高度通用的网络安全水平”的机构，根据欧盟 2019 年《网络安全法案》的规定，负责指导制定欧盟网络安全认证框架的技术标准和政策。可以预见，隐私增强技术将成为欧盟重点关注领域。

（二）美国发布法案支持隐私计算技术的研究与使用

2019 年 12 月，美国白宫行政管理和预算办公室（OMB）发布《联邦数据战略与 2020 年行动计划》。以 2020 年为起始，联邦数据战略描述了美国联邦政府未来十年的数据愿景，将“数据作为战略资源开发”的核心目标，提出着重改进特定数据资源组合的管理和使用。美国对数据的关注重点从“技术”向“资产”转移，致力于打造数据资源集中化利用与配置。

2019 年，美国共和党提交《2019 美国国家安全与个人数据保护法案》，以保护本土企业和国民数据为切入口，限制跨境数据流向，从微观层面控制数据的传输和存储，具有鲜明的、针对其他

国家的数据保护意识。随后，拜登政府宣告对美国进行有意义的联邦隐私改革。美国众议院和参议院制定了《促进数字隐私技术法案》（S.224）以“支持隐私增强技术的研究，并促进负责任的数据使用”。如果通过，该法案还将授权美国国家科学基金会（NSF）促进对隐私增强技术的研究，并制定标准促进隐私增强技术在公共和私营部门数据使用中的作用。

（三）英国设立国家机构研究隐私计算技术并促进应用

英国于 2018 年成立数据伦理与创新中心（CDEI）。该机构持续研究隐私增强技术在实现安全、私有和可信赖数据使用中的作用，重点方向包括同态加密、可信任执行环境、多方安全计算、联邦学习、差分隐私等。2020 年 7 月，CDEI 发布《解决对公共部门数据使用的信任问题》报告，指出隐私增强技术更好地保护不同数据共享方法的隐私和安全性。2020 年 12 月，英国发布国家数据战略，以提高使用私有和共有数据的访问效率和公众信任，其中提及将探索隐私增强技术支持个人数据保护，加强公众对如何使用数据的控制，进而增强公众信任。疫情期间，英国使用 OpenSAFELY 安全分析平台，通过隐私增强技术对 2400 万患者的记录进行分析，识别与新冠疫情相关的危险因素。

第二章 技术篇

隐私计算从技术机制上分为三大类：基于协议规则的技术，包括多方安全计算、联邦学习、可证去标识；基于算法的差分隐私；基于硬件环境的机密计算。各方向技术特点不同（如图 1 所示），适用于不同场景：基于密码学的多方安全计算及同态加密等方法更适用于数据量适中但保密性要求较高的重要数据应用；联邦学习更适用于保密性要求不高但数据量大的模型训练；差分隐私能够减少计算结果对隐私的泄露，但会降低结果的准确性，一般与其他技术结合使用；机密计算则因为性能优势而更适用于复杂、数据量大的通用场景和通用算法，如大数据协作、人工智能框架数据保护、关键基础设施保护等，但是目前的安全性受限于硬件的设计与实现；可证去标识同样适用于数据量大、实时性要求高、数据出域的应用场景。

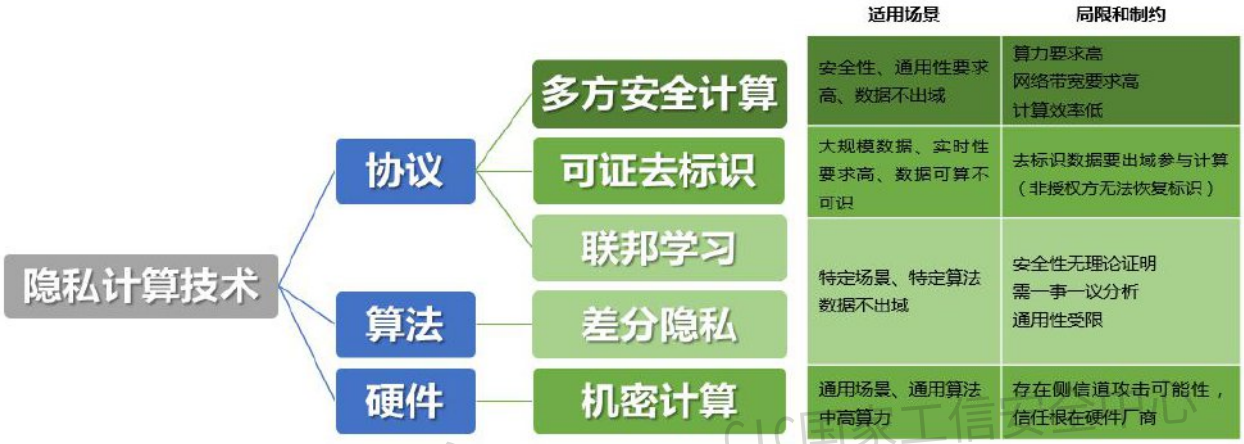

图 1 隐私计算技术体系

来源：国家工业信息安全发展研究中心

虽然目前隐私计算性能已经大大提升，但加密机理复杂、交互次数多，当流通的数据量较大或结构较为复杂时，计算效率问题仍然未能解决。特别是对于复杂算法的联合建模效率仍然难以

令人满意。当前，关于多方安全计算、联邦学习、差分隐私、去标识、防身份关联等技术理论基础研究已相对成熟，但隐私保护技术的技术成熟度和产业化能力尚弱。现阶段，项目实施方面对于隐私计算技术产品及服务的选择是以落地实际需求为牵引。即各方的信任度越高，隐私计算方案支撑的计算效率越高；反之，若设定其中某方完全不可信，则隐私计算的效率低，难以满足大规模商用要求。

一、多方安全计算

多方安全计算（Secure Multi-Party Computation），MPC 由姚期智在 1982 年提出，主要探讨保障隐私的前提下，多个参与方各自输入信息计算一个约定的函数。海量数据交叉计算的特性使多方安全计算可以为科研、医疗、金融等提供更好支持。许多企业或组织出于信息安全或利益的考虑，内部数据是不对外开放的，数据的价值无法体现或变现。多方安全计算（MPC）可以很好解决这一难题。保证各方数据安全的同时，又得到预期计算的结果。

图 2 多方安全计算发展

来源：国家工业信息安全发展研究中心

（一）技术简介

多方安全计算是指参与者在不泄露各自隐私数据情况下，利用隐私数据参与保密计算，共同完成某项计算任务。该技术能够满足人们利用隐私数据进行保密计算的需求，有效解决数据的“保密性”和“共享性”之间的矛盾。多方安全计算包括多个技术分支，目前，在 MPC 领域，主要用到的是技术是秘密分享、不经意传输、混淆电路、同态加密、零知识证明等关键技术。

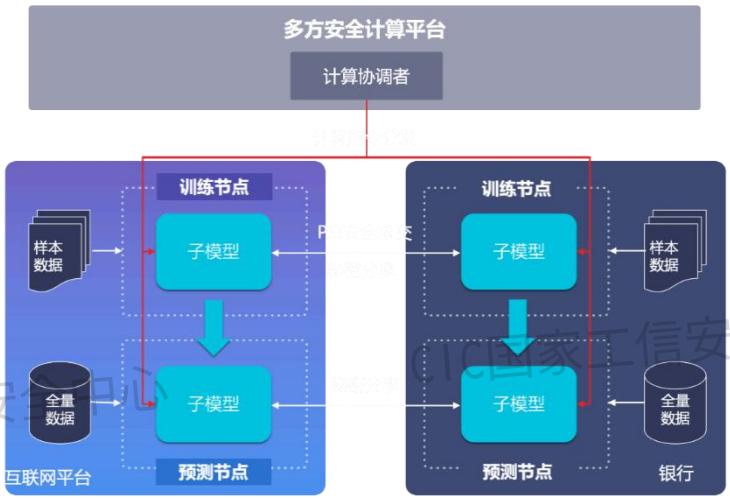

图 3 多方安全计算模式

来源：国家工业信息安全发展研究中心

1. 秘密分享

秘密分享是指将秘密以适当的方式拆分，拆分后的每一个份额由不同的参与者管理，每个参与者持有其中的一份，协作完成计算任务（如加法和乘法计算）。单个参与者无法恢复秘密信息，只有若干个参与者一同协作才能恢复秘密消息。由于秘密分享具有计算同态性质，每个参与者可以独立的基于分片的数据进行加法和乘法计算，各个参与者将计算的分片结果发送给结果方进行汇总还原出计算结果。整个过程中各个参与者不能获得任何秘密信息，结果方只能获取结果信息，因而有效地保护原始数据不泄

漏，并计算出预期的结果。在秘密共享系统中，攻击者必须同时获得一定数量的秘密碎片才能获得密钥，系统的安全性得以保障。另一方面，当某些秘密碎片丢失或被毁时，利用其它的秘密份额仍能够获得秘密信息，系统的可靠性得以保障。

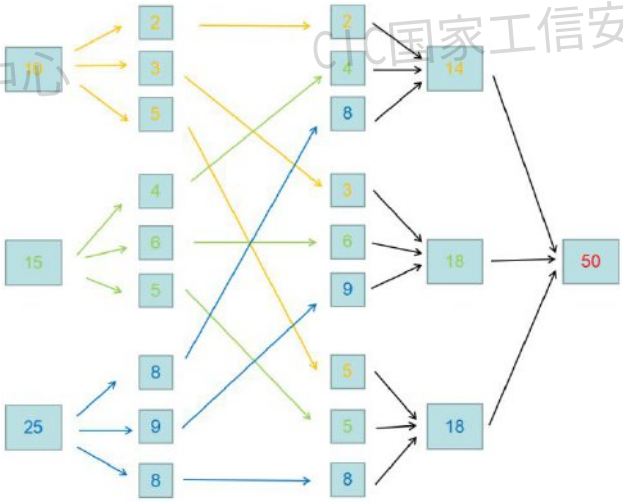

图 4 秘密分享原理

来源：国家工业信息安全发展研究中心

2.同态加密

同态加密是一种允许在加密之后的密文上直接进行计算，且计算结果解密后和明文的计算结果一致的加密算法。在多方安全计算场景下，参与者将数据加密后发送给统一的计算服务器，服务器直接使用密文进行计算，并将计算结果的密文发送给指定的结果方。结果方再将对应的密文进行解密后，得出最终的结果。过程中保证计算服务器一直使用密文进行计算，无法查看到任何有效信息，而参与者也只能拿到最后的结果，无法看到中间结果。按照支持的功能划分，同态加密方案可以分为部分同态加密和全同态加密。部分同态加密是指支持加法或者乘法运算，全同态加密是指同时支持加法和乘法运算的加密算法。当前部分同态加密

技术已经比较成熟，但是全同态加密方案在性能方面仍然与实际应用的要求存在一定距离，因此实际应用较少。

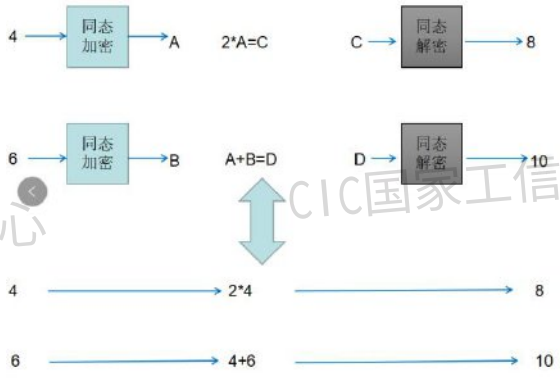

图 5 同态加密原理

来源：国家工业信息安全发展研究中心

3.不经意传输

不经意传输是一种可保护隐私的双方通信协议，消息发送者从一些待发送的消息中发送某一条给接收者，但并不知道接收者具体收到了哪一条消息。不经意传输协议是一个两方安全计算协议，协议使得接收方除选取的内容外，无法获取剩余数据，并且发送方也无从知道被选取的内容。不经意传输对双方信息的保护可用于数据隐私求交场景。通过不经意传输，参与双方不能获取到对方的任何数据信息，结果方仅仅只可以获取到交集数据。

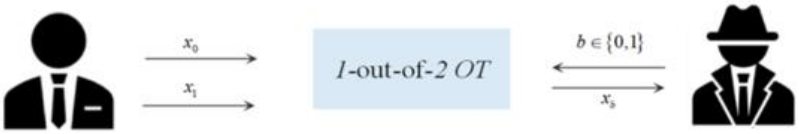

图 6 不经意传输原理

来源：国家工业信息安全发展研究中心

4.混淆电路

混淆电路是双方进行安全计算的布尔电路。混淆电路将计算电路中的每个门都加密并打乱，确保加密计算的过程中不会对外泄露计算的原始数据和中间数据。双方根据各自的输入依次进行

计算，解密方可得到最终的正确结果，但无法得到除结果以外的其他信息，从而实现双方的安全计算。

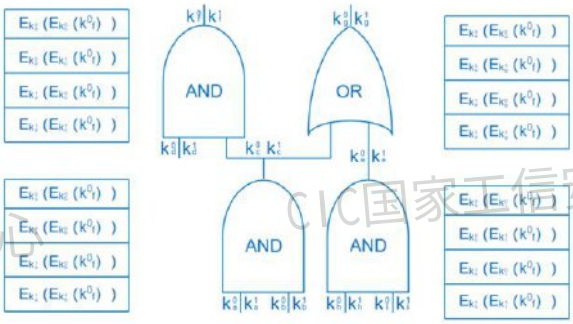

图 7 混淆电路原理

来源：国家工业信息安全发展研究中心

5.零知识证明

零知识证明指的是证明者能够在不向监控者提供任何有用信息的情况下，使验证者相信某个论断是正确的。零知识证明实际上是一种涉及双方或更多方的协议，即双方或更多方完成一项任务需要采取的一系列步骤。证明者需要向验证者证明并使其相信自己知道或拥有某一消息，但证明过程不向验证者泄露任何关于被证明消息的信息。例如，网站将用户密码的 Hash 散列值储存在 web 服务器中。为了验证客户端是否真的知道密码，要求客户端输入密码的 hash 散列，并将其与储存的结果进行比较。

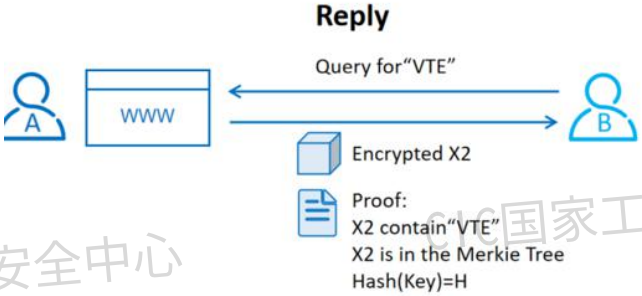

图 8 零知识证明原理

来源：国家工业信息安全发展研究中心

（二）技术优缺点

多方安全计算理论已经提出近40年，出现多个技术分支。基于多方安全计算理论研究，技术实现层面也取得了较大进展，开源系统框架和工具覆盖多种理论技术，不断推进多方安全计算的计算性能，不断接近工程应用的实际水平。

从技术范畴和应用范围看，多方安全计算能够实现多方数据安全融合，存在很多横向的类似技术和成果。除安全多方技术外，数据安全融合相关技术主要有数据脱敏、差分隐私、可信执行环境、联邦学习等。从安全性、计算准确性、计算性能以及通用性（应用场景和领域）等角度进行相比，以上技术各有利弊：**数据脱敏**技术的计算性能高，适用于大数据量处理，但其可追溯性差，数据脱敏后的去向和使用难以从技术上有效控制。**差分隐私**技术通过增加噪声来保护数据隐私，计算性能也很高，但噪声带来的偏差使得结果准确性降低。**可信执行环境**为程序、数据提供了一个安全可靠的环境，其性能及通用性具有较大优势，但信任链绑定CPU厂商，且理论上存在侧信道攻击的可能性。**联邦学习**通过数据不出本地、只交换中间模型参数的方式实现多方安全建模。联邦学习技术的安全性基于相信无法通过中间模型参数推断出原始数据，但此结论没有密码学保证，因此联邦学习需要和其他密码技术结合来保证安全性。与上述技术相比，**多方安全计算**基于密码学安全，其安全性有严格密码理论证明，不以信任任何参与方、操作人员、系统、硬件或软件为基础，同时计算准确度高，并支持可编程通用计算。

目前多方安全计算面临以下问题：从技术上看，计算性能问

题是应用的一大障碍。随着应用规模扩大，采用合适的计算方案保证运算时延与参与方数量呈现线性变化是目前各技术厂商面临的一大挑战。目前，多家技术厂家正在研究采用硬件设备进行运算加速。从安全性上看，多方安全计算的目标是保证多方数据融合计算时的隐私安全，一些传统安全问题，如访问控制、传输安全等，仍然需要其他相应的技术手段。

（三）国内主要厂商

1.蚂蚁集团

蚂蚁集团旗下多方安全计算平台是一套自主研发的工业级分布式高性能的多方安全计算智能应用平台，具备功能丰富扩展性强的多方安全算子库和多方安全计算的高效机器学习算法库，可以实现多方安全联合建模、联合分析、联合规则。平台已规模化在金融行业中实践，赋能数十家金融机构实现联合风控。

2.华控清交

华控清交是于2018年由清华大学发起组建的专注于研究隐私计算等数据安全技术的企业，是目前业界唯一一个有强大学术基础及后续补充的科技企业。华控清交以基于密码学的多方安全计算为核心，结合数据脱敏、差分隐私、联邦学习和可信计算等基于明文计算的数据隐私保护技术和区块链，创建了一套具有强横向扩展性、高并行计算性能、便于监管的数据融合与流通平台，可以同时支持隐匿查询、联合统计、联合建模和数据跨境等数据应用需求。

3.富数科技

富数科技定位于企业级安全计算平台，自主研发本地化安全计算平台——Avatar，从功能上集成富数科技多方安全计算、联邦学习、匿踪查询、联盟区块链等四大核心技术能力，解决包括本地化部署、联合统计、联合建模、联合营销、查询不留痕等行业需求，实现完全本地化平台产品交付。

（四）应用场景与案例

1.投资人资格认证（隐匿查询）

金融机构放款前须对借款人的资质、资产情况进行审核，避免金融风险。传统方式采用线下人工审核借款人/投资人资格，用户耗时耗力、结果无法通用。借助于多方安全计算，实现基于行业内可信的数据平台，通过秘密分享或者不经意传输技术，实现隐匿查询功能，从而即保证各个金融机构数据的安全性，也对查询人员信息进行了保护。具体而言，查询方采用多方安全计算，隐藏被查询对象关键词或客户 ID 信息，数据提供方匹配查询结果却无法获知具体对应哪个查询对象，同时保护查询方的查询意图和数据提供方的数据。数据不出域，杜绝数据缓存、数据泄漏、数据贩卖的可能性。

2.联合统计

各参与方数据对其它方和多方计算平台保密，查询结果方只得到统计信息，无统计的算法参数等其他信息。统计方通过多方计算平台查询一个或多个数据提供方的数据库，得到查询统计结果，统计结果与在明文数据库上查询的结果一致。例如，某电力行业监管机构统计某工业电力数据总量。利用多方安全计算平台，

通过秘密分享、同态加密等技术，实现安全的联合统计，保障上市企业不提前披露数据。在保险行业中，通过多方安全计算可实现医疗保险公司与医疗机构间对理赔标准进行分析，在保障用户隐私的前提下实现合理的理赔标准制定以及理赔的线上智能风控。

二、联邦学习

2016 年，谷歌提出联邦学习，使安卓手机终端用户在本地更新模型，随后因为其有效的解决数据孤岛问题而被大力推广。联邦学习最大的价值在于改变了数据资源的拥有和联合方式，目前广泛应用于提升人工智能网络模型能力。国外联邦学习起步较早，已形成商业化产品，例如，谷歌的 TensorFlow Federated、英伟达的 Clara FL 等。国内厂商方面，2020 年通过评测的联邦学习产品多达 18 款，包括微众银行推出的工业级联邦学习框架 FATE 等。目前拥有联邦学习平台和产品的企业已经超过 60 多家，涉及各类企业，由此可见联邦学习在隐私计算领域的应用正在不断扩大。

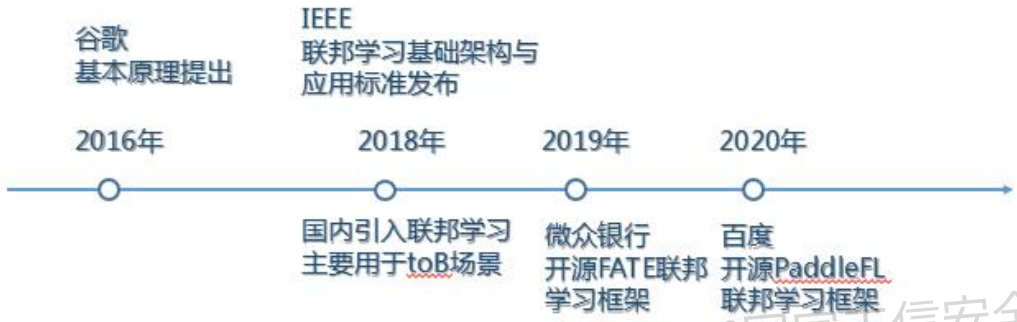

图 9 联邦学习发展

来源：国家工业信息安全发展研究中心

（一）技术简介

联邦学习的本质是一种机器学习框架，即分布式机器学习技术。联邦学习以一个中央服务器为中心节点，通过与多个参与训练的本地服务器（以下简称“参与方”）交换网络信息来实现人工智能模型的更新迭代，即中央服务器首先生成一个通用神经网络模型，各个参与方将这个通用模型下载至本地并利用本地数据训练模型，将训练后的模型所更新的内容上传至中央服务器，通过将多个参与方的更新内容进行融合均分来优化初始通用模型，再由各个参与方下载更新后的通用模型进行上述处理，这个过程不断重复直至达到某一个既定的标准。在整个联邦学习的过程中，各参与方的数据始终保存在其本地服务器，降低了数据泄露的风险。

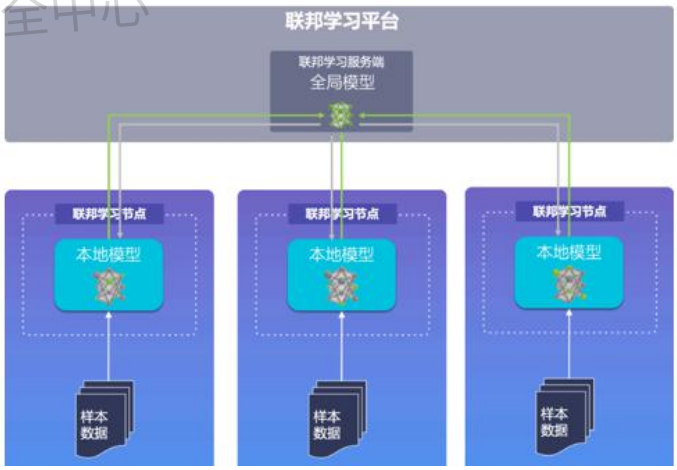

图 10 联邦学习模式

来源：国家工业信息安全发展研究中心

联邦学习根据不同参与方的数据特点，可分为三类：

1.横向联邦学习

横向联邦学习适合样本数据的特征重合较多，但数据量较少的场景，即各个参与方的业务逻辑相似，但是用户不重合。例如，

银行行业与保险行业中，不同企业或不同地区的同行业的业务逻辑是相同的，但是用户不重合。故横向联邦学习是以样本联合为基本思想来进行模型训练。

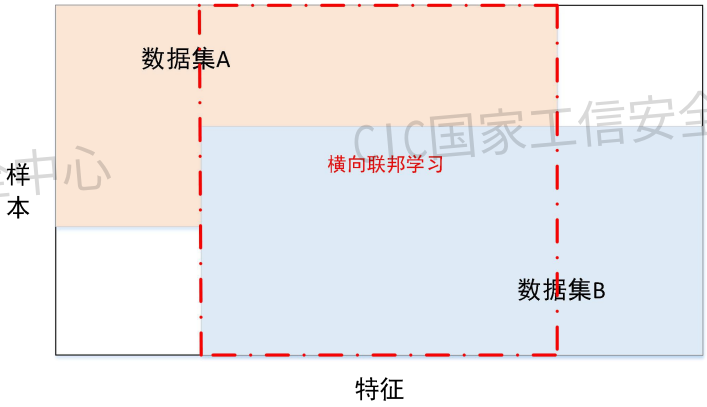

图 11 横向联邦学习

来源：国家工业信息安全发展研究中心

在横向联邦学习中，各个参与方从中心服务器下载初始或当前最新的通用模型，利用本地数据对模型进行训练，并将加密后的模型梯度返回到中心服务器，服务器依据各参与方返回的数据对现有通用模型进行更新之后，各参与方再重新利用新的模型进行训练。

2.纵向联邦学习

纵向联邦学习适合各参与方的样本数据重叠多，但样本数据特征重叠较少的场景，即各个参与方的用户相似，但是业务逻辑不同的情况。例如同一地区的银行行业和零售行业，本质上各自的用户都是该地区的居民，但他们的业务逻辑不同。故纵向联邦学习是以重叠用户在不同业务逻辑下的特征联合为基本思想来进行训练的。

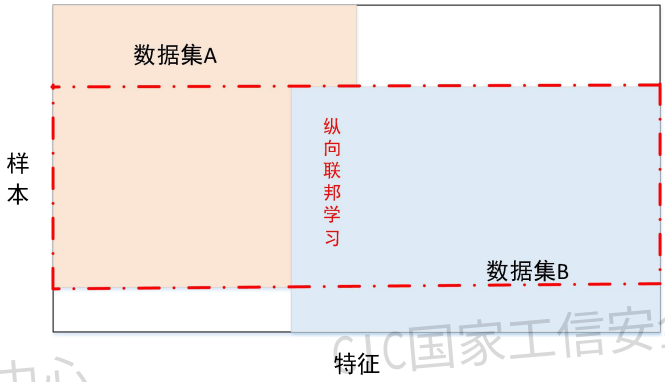

图 12 纵向联邦学习

来源：国家工业信息安全发展研究中心

纵向联邦学习首先将各参与方所参加训练的样本进行加密对齐，再进行训练。由中心服务器向各参与方发送公钥，这个公钥用来加密各节点与中心服务器中所需传输的数据，各参与方从中心服务器下载初始模型进行训练，将模型的梯度使用私钥加密传输至中心服务器，在中心服务器聚合各参与方返回的数据将模型更新之后，各参与方下载更新结果并解密，再进行下一轮训练。

3.联邦迁移学习

联邦迁移学习适合各参与方的样本数据重叠较少，同时样本数据特征也重叠较少的场景。即各个参与方的用户重叠较少，业务逻辑也不同的情况。例如不同地区的不同行业，其面向的用户是不同的，所完成的业务也是不同的。故联邦迁移学习是以源领域和目标领域之间的相似性为基本思想进行模型训练的。

联邦迁移学习要求各参与方在样本加密对齐的基础上对各自的梯度、权重及损失进行计算，通过加密上传至中心服务器，中心服务器基于上传的数据进行聚合并调整通用训练模型，各参与方下载并解密进行训练。

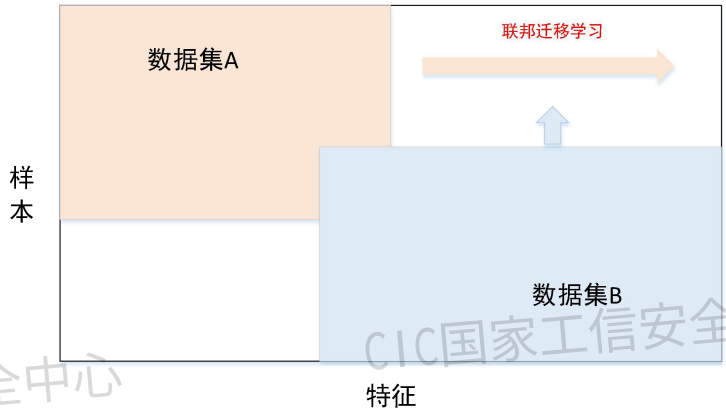

图 13 联邦迁移学习

来源：国家工业信息安全发展研究中心

（二）技术优缺点

联邦学习所解决的根本问题是从参与训练的数据量着手来提升神经网络模型的性能。联邦学习提出之前，业内通常从收集与产生更多的数据、对数据进行缩放、变换及选择更优的特征四个方面来提升算法性能，即从已有数据出发，增加现有数据的质量及复用性来提升神经网络模型性能。但提升整体模型算法性能投入较大，一方面是不同算法对软硬件需求不同，另一方面是普适优秀的算法产出难度较大。一般来说，当数据特征相似时，神经网络的模型性能与数据量和数据质量成正比，但由于公开数据集体量不足，导致模型训练期的数据投喂量不足，使得模型性能不够优秀，只能解决与当前参训数据特征相似的数据场景，这些模型市场应用效果较差。另外，业内也通过数据的整合及购买等手段尝试解决这类问题，但单次训练的数据量巨大，对算力提出了更高的要求，因此在算力不足的情况下同样不能高效的训练出性能较好的模型。与原有方案对比，联邦学习由于其具有分布式训练和联合训练的特点，一方面能够解决训练阶段数据特征单一的

问题，从而获得一个性能更好的、优于利用自己本身数据集所训练出的模型。另一方面，各参与方只需在本地利用各自数据集进行训练，数据体量未增加，算力成本压力小。因为整个训练过程中各参与方的数据都不会离开本地，只将模型的梯度及权重等信息上传至中心服务器进行聚合分割，对于各参与方来说这样既不会直接泄露隐私数据，也不会额外增加参训数据量，从而完成训练任务。

但当下只依靠联邦学习依然存在着安全问题。从训练机制看，关键步骤在于中心服务器聚合及分发神经网络梯度及权重等信息。一是就目前业内应用较大的神经网络模型来看，因为从底层编码开始构建一个基础的神经网络模型通常耗时耗力，多数企业从开源平台获取或第三方平台上购买基础模型，这样的基础模型本身就有植入病毒的可能。二是利用中心服务器收集的梯度及权重信息能够反推出每个参与方的数据信息。三是联邦学习的机制默认所有参与方都是可信方，无法规避某个参与方恶意提供虚假数据甚至病害数据，从而对最终的训练模型造成不可逆转的危害。针对上述联邦学习存在的安全问题，首先可以考虑由一个公认可信方负责提供基础的神经网络模型。其次，在中心服务器进行梯度及权重等信息聚合分发时，结合基于密码学的加密方式，例如同态加密、差分隐私等，对各参与方上传的信息进行二次加密以保证无法通过梯度、权重等信息进行反推。最后，针对现存可信方形成一个联邦学习的生态圈和相应的黑名单，并引入激励惩罚机制，以此来保证生态圈内的参与合作方都为可信方。

（三）国内主要厂商

1.微众银行

微众银行是国内最初提出联邦学习概念并将其应用于企业产品中的团队。旗下基于联邦学习技术的贷款服务平台一方面通过联邦学习所训练的推荐模型提高产品推广的精准度，另一方面通过安全风控模型把控用户的信用评级和授信额度，以提高金融产品的盈利率。由于微众银行由腾讯内部孵化，与国内其他基于联邦学习技术的金融厂商相比，用户基数群构成了其较大的数据优势。

2.蚂蚁集团

蚂蚁集团旗下蚂蚁隐私计算智能服务平台基于自主研发Fascia联邦学习开发框架与多方安全计算、差分隐私等技术结合实现更安全的联邦学习产品，可实现联合统计、联合建模。在医疗行业中，联合阿里云已与大型跨国医疗企业合作应用在疾病诊断、检查推荐、用药推荐、罕见病预测、质控规则管理等场景中，为医疗数据治理、全院质控、医学研究、医保风控和临床核心业务中的痛点难点问题提供解决方案。

3.翼方健数

翼方健数是一家以隐私计算和人工智能为主要研究方向，以多方安全计算及联邦学习为主要技术手段的平台服务型企业。2019年初发布数据医疗隐私计算平台XDP翼数坊。旗下系列产品PathFinder、Pioneer、Percepter主要着力于解决智慧医疗生态下的各类现存问题，包括联邦学习赋能病历的自主学习，传染病的防控模型及疾病的病灶图像识别等。

4.数牍科技

数牍科技是于2019年组建的基于联邦学习及多方安全计算技术的技术服务公司，旗下产品Sodu当前主要服务于银行业，用于用户获取及信用评估场景，为银行各系列金融产品提供更精准的用户群和相对应的信用等级指标。

5.锘崴科技

锘崴科技是一家以隐私计算和医学基因为主要研究方向的大数据隐私计算平台公司。旗下的产品锘崴信基于联邦学习技术为业界提供了一个数据价值合作流动生态，以数据的价值提供方和价值使用方为主要参与者，打造数据可用不可见、数据价值流通的服务平台。

（四）应用场景与案例

联邦学习因其满足“数据可用不可得”的特点，使其能够在大量需要数据支撑的行业得以应用。从国内现有厂商和其产品来看，金融与医疗行业是目前应用最多的方向。此外，增量市场主要体现在以下几个方面：一是应用于工业领域，主要保障仓储及物流的数据安全性。二是应用于车联网及自动驾驶领域，提高单个车辆节点对交通风险的识别和规避能力，更能提高整个自动驾驶网络的安全性。三是应用于智慧城市，联合多行业进行安防系统的共同构建，形成高防控能力的风控模型。

1.医疗行为分析

医疗行业中面向医疗机构与相关企业基于联邦学习技术进行联合建模的落地应用。例如，多家医疗机构以性别、年龄等数据

特征及患病与否等标签，采用横向联邦学习联合开展一项某项疾病的因素分析。此外，医疗机构与医保局通过同一用户群的支付数据、医院就诊数据、金融信用数据，采用纵向联邦学习联合分析医保欺诈。一般情况下，联邦学习训练的模型性能可达到集中式训练水平。

2.信用风险防控

金融行业中面向金融机构与政府基于联邦学习技术进行联合建模的落地应用。例如金融机构结合其服务企业的金融行为、资产等特征与政府的企业信息、企业税务信息、企业违规信息等特征，采用纵向联邦学习联合建模开展企业的信用风控评估。金融机构间通过同一用户群的金融行为数据采用纵向联邦学习联合分析金融反欺诈。

三、差分隐私

差分隐私技术自 2006 年提出后经历了从单纯的理论研究阶段到目前实际应用反哺理论研究阶段。其相对传统密码学，具有计算复杂度低的优势，目前差分隐私进入了具备完备的基础原理，在实际应用中根据需要不断探索技术边界的阶段。

图 14 差分隐私发展

来源：国家工业信息安全发展研究中心

（一）技术简介

差分隐私是基于信息论和概率论的一门学科，提供一种从统计数据库查询，最大化数据查询的准确性，同时最大限度减少识别查询记录的方法。差分隐私的隐私保护程度较高，满足差分隐私的数据集能够抵抗任何对隐私数据的攻击，即攻击者根据获取到的部分数据信息并不能推测出全部数据信息。基于差分隐私保护的数据发布是差分隐私研究中的核心内容。传统的差分隐私，即中心化差分隐私，将各方的原始数据集中到一个可信的数据中心，对计算结果添加噪音。但由于可信的数据中心很难实现，因此出现了本地差分隐私。本地差分隐私为了消除可信数据中心，直接在用户的数据集上做差分隐私，再传输到数据中心进行聚合计算，数据中心也无法推测原始数据，从而保护数据隐私。

目前差分隐私技术已经被谷歌和苹果广泛应用于 IOS 系统和 Chrome 系统中，虽然这项技术仅发展了十年，但其应用覆盖面不仅包括计算机和手机的操作系统，也包含业内金融及医疗的大多数场景中，使用差分隐私可以在保护数据隐私的前提下进行数据的查询分析等操作。

（二）技术优缺点

在差分隐私算法提出之前的数十年里，学术界一直在探索数据分析中的隐私保护技术，包括 k-匿名，I-多样化等。但是这些技术都有局限性和相应的攻击手段。微软科学家 Cynthia Dwork 在 2006 年提出了“差分隐私”，从信息论的角度给出了严格的隐私泄露的定义。以此为基础，学术界提出一系列差分隐私的算法和

系统，针对不同的应用场景来降低隐私的泄露。从差分隐私机制角度，针对不同需求提出了诸如拉普拉斯机制、高斯机制、随机响应机制、指数机制、稀疏向量等经典差分隐私保护机制。为了减小对数据查询、函数计算结果的影响，减小差分隐私引入的噪声功率、阶梯机制、截断拉普拉斯等机制也相继被提出。另外，针对数据相关性等影响，高斯矩阵机制等一些新的机制也相继提出。为了减小差分隐私对性能的损失，研究人员根据不同需要提出了针对不同场景的隐私放大方案，例如，基于采样的隐私放大、基于迭代的隐私放大、基于改组的隐私放大等。同时，对于多次的查询和迭代计算，进一步提出了差分隐私界和相应的中心极限定理。

差分隐私技术不仅作为一个独立的技术方向得到深入的研究，又与深度学习、联邦学习、多方安全计算等方向深度耦合。例如为联邦学习和深度学习提供隐私保护。由于其对性能的影响，也催生了对联邦学习、深度学习中适应差分隐私保护的特别的框架和模型的研究，在多方安全计算中，采用可计算的差分隐私能大大降低多方安全计算的计算复杂度和通讯量。但就目前多个研究，差分隐私由于其技术机制原理，算法输出结果并不精确，学术界还在进行更高效的差分隐私技术研究。

（三）国内主要厂商

1.蚂蚁集团

蚂蚁集团旗下隐私计算智能服务平台将差分隐私与多方安全计算、联邦学习技术结合，实现全链路的计算隐私保护，已在医

疗行业的联合诊断增强中进行探索性应用。

（四）应用场景与案例

1.推荐系统

推荐系统用于帮助企业或用户从大量数据中寻找可能需要的信息，需要利用大量用户数据进行协同过滤。在基于差分隐私的推荐系统中，数据中心利用局部差分隐私，将处理之后的数据集上传到数据中心进行聚合计算，将获得相同计算结果的数据反馈给用户。以此达到在不泄露隐私数据的前提下完成推荐行为。

2.网络踪迹分析

行业研究的机构、政府治理监管部门通过网络数据和流量记录数据对行业的发展状况进行分析及研究。差分隐私技术可以将用户的网络踪迹，包括但不限于浏览记录、用户习惯、使用时长、下载记录等进行保护处理。

四、机密计算

自 Intel 2015 年发布 Intel SGX 以来，机密计算发展日益加速，涌现出越来越多的新技术和新产品（见下图）。机密计算技术是通过在基于软硬件的可信执行环境（Trusted Execution Environment，TEE）中执行计算，保护数据和应用，达到隐私计算效果的技术。机密计算结合安全传输和安全存储等传统技术，可实现包含传输、存储、计算在内的全周期数据隐私保护。相对于其他隐私计算技术，机密计算具有通用和高效的特点，不仅可以无缝支持通用计算框架和应用，而且计算性能基本可匹敌明文计算（比如正常的

Linux 计算应用）。因此，机密计算的应用范围极为广泛，尤其对于安全可信云计算、大规模数据保密协作、隐私保护的深度学习等涉及大数据、高性能、通用隐私计算的场景，更是不可或缺的技术手段。

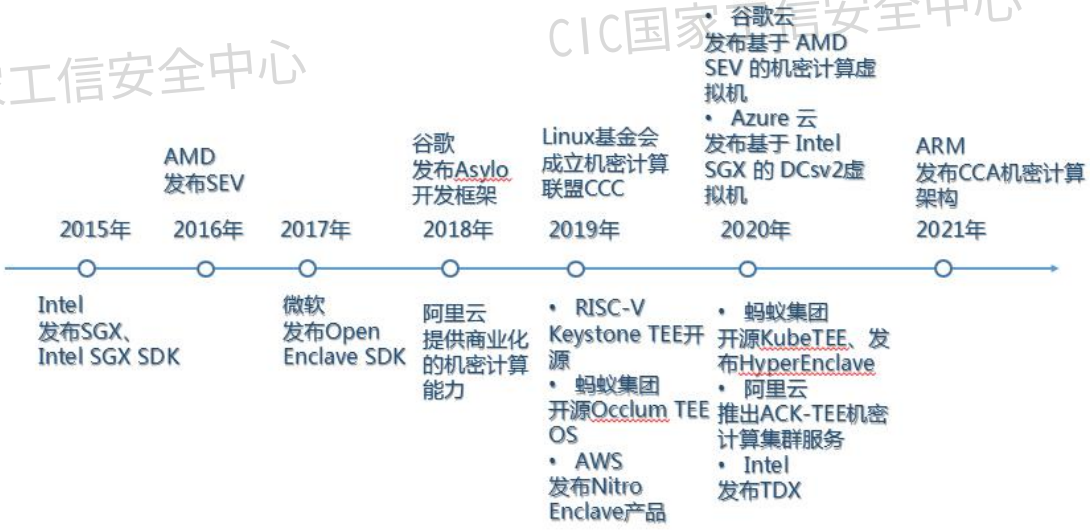

图 15 机密计算发展

来源：国家工业信息安全发展研究中心

机密计算的实施依托 TEE 的软硬件实现和 TEE 的支撑软件。TEE 实现方面，目前主流的 CPU 厂商都提供了 TEE 实现，比如 Intel SGX、AMD SEV、Intel TDX、ARM Realm 等；一些国产 CPU 也提供了颇具竞争力的 TEE 实现，比如 x86 CSV。值得一提的是，近来出现的软硬结合的 TEE 实现（如蚂蚁集团研发的 HyperEnclave），在充分利用 CPU 的内存加密能力的同时，将信任根从 CPU 卸载到外置可信模块，可以让用户对 TEE 信任链具有更强的掌控力和自主性，缓解了对于 TEE 信任链和 CPU 硬件厂商绑定的担忧。

TEE 支撑软件方面，目前已经形成了比较完整的 TEE 软件栈，大致分为三类：TEE SDK（如 Intel SGX SDK、Open Enclave SDK）、

TEE OS（如 Occlum）、TEE 集群软件（如 KubeTEE）。

（一）技术简介

机密计算是一种通用高效的隐私计算技术，其通过隔离、可信、加密等技术，可对数据加密处理，保障使用中数据（Data-in-use）的机密性和完整性。

TEE 作为机密计算的支撑技术，一般需实现如下四个技术目标的一个或多个：隔离执行、远程证明、内存加密、和数据封印。其中，隔离执行是通过软硬结合的隔离技术将 TEE 和非 TEE 系统隔离开来，使得可信应用的 TCB（Trusted Computing Base，可信计算基）仅包含应用自身和实现 TEE 的基础软硬件，而其他软件甚至是操作系统内核这样的特权软件都可以是不可信的甚至是恶意的。远程证明支持对 TEE 中代码进行度量，并向远程系统证明的确是符合期望的代码运行在合法的 TEE 中；内存加密用于保证在 TEE 中代码和数据在内存中计算时是处于加密形态的，以防止特权软件甚至硬件的窥探；而数据封印可用于从 TEE 将数据安全地写入外部的永久存储介质，且该数据仅能被相关 TEE 再次读入。Intel SGX 是目前应用最广泛的 TEE，它完整实现了上述四个技术目标；而 HyperEnclave 结合 CPU（含国产 CPU）的内存加密能力，也完整实现了上述四个目标。一些 TEE 如 ARM TrustZone 等则仅实现了部分目标。

从 TEE 软件支撑技术来看，现有 TEE SDK 要求开发者采用二分式开发方法分割应用并设计好各部分的接口，其基础库所支持的 API 非常有限且仅支持 C/C++等编程语言，难以支持多数应用

或算法框架也不能适应业界对于多种编程语言的需求。与其对比，2019 年开源的 Occlum 和 2016 年开源的 Graphene，作为机密计算联盟的官方 TEE OS 项目，可兼容 Linux 环境的 API，使现有应用几乎不需分割或改造，即可运行于可信执行环境，大大降低了 TEE 应用开发门槛。TEE OS 也支持多语言，例如，Occlum 除了 C/C++ 之外，还支持几乎所有主流编程语言，如 Python、Java、Go、Rust、JS 等，从而能支持主流 AI 或大数据框架。安全性上，Occlum 用内存安全语言 Rust 开发，可排除大部分内存安全问题，且提供了加密文件系统及加密镜像的支持。TEE 集群支持将 TEE 和现代集群软件如 Kubernetes 有机结合。开源软件 KubeTEE 实现了 TEE Device Plugin，使得 TEE 节点可以纳入 Kubernetes 的统一伸缩和容错框架，同时利用 TEE 特有的远程证明机制支持集群规模的远程证明和密钥管理。

在 TEE 支撑软件方面，国内外厂商基本处于同一水平，且出于增强可信度的需要，基本都采用了开源软件的形式。目前在该领域领先的、在国内外均有较多用户的 Occlum TEE OS、KubeTEE、Rust TEE SDK 都是由国内公司发起的开源项目。另外，开源的 Intel SGX SDK 的主力开发人员也是国内团队。在 TEE 应用软件方面，国内对于应用场景的探索更加深入和落地，比如在区块链隐私保护、数据协作、联合风控、隐私保护的大数据处理系统有丰富的应用案例。

（二）技术优缺点

机密计算相对于其他隐私技术的优势在于它兼顾了安全性、通用性、和高效性。相对于其他隐私计算技术，机密计算具有通用和高效的优势，不仅可以无缝支持通用计算框架和应用，而且计算性能基本可匹敌明文计算。它可以单独用于隐私计算，也可以与其他技术结合在一起来保护隐私，尤其对于安全可信云计算、大规模数据保密协作、隐私保护的深度学习等涉及大数据、高性能、通用隐私计算的场景，是重要的技术手段。

一般认为,机密计算的缺点在于TEE信任链跟CPU厂商绑定，从而影响到机密计算技术的可信度。机密计算的另一个缺点是目前的 TEE 实现在理论上存在侧信道攻击的可能性。针对第一个缺点，近年来业界涌现出了基于虚拟化技术将信任链跟 CPU 解耦的解决方案，比如微软的 VSM（Virtual Secure Mode）、AWS 的 Nitro Enclave 等。国内厂商蚂蚁推出的 HyperEnclave，进一步将信任根从 CPU 卸载到外置可信模块并托管到国家权威机构，只借用 CPU 的内存加密硬件能力，实现了软硬结合、灵活自主、不依赖 CPU 厂商可信性的 TEE 方案。针对第二个缺点，业界一般通过及时更新固件、随机化、Data oblivious 系统设计等多种手段来缓解。

（三）国内主要厂商

1.蚂蚁集团

研发了结合虚拟化隔离技术和可信平台模块技术的新型 TEE 技术 HyperEnclave，支持由用户自主掌控 TEE 信任根；HyperEnclave 可集成国内外内存加密硬件引擎，实现各项 TEE 技

术目标。蚂蚁集团开源了 Occlum 项目，并捐赠给机密计算联盟成为联盟官方产品。

2.阿里云

阿里云在 2018 年提供商业化的机密计算能力，在 2020 年推出了 ACK-TEE 机密计算集群服务。

3.百度

百度是国内较早布局隐私计算产业的企业。百度点石联合建模平台基于 Intel SGX 可信执行环境，结合联邦学习、多方安全计算、隔离域、区块链等技术能力，提供一站式企业级可信数据安全协作解决方案，满足营销、金融、医疗、政务等场景的业务需求。

4.翼方健数

翼方健数以隐私安全计算为核心，在数据安全和隐私保护基础上提供数据开放共享协作的环境。旗下推出的隐私安全计算平台 XDP 翼数坊，融合英特尔 SGX 技术“机密计算”能力，与英特尔联手发布的多模态隐私保护解决方案在任务处理、算法拓展性、计算机密性、一致性方面性能突出。目前主要为医疗健康、政府数据共享提供隐私计算基础设施。

（四）应用场景与案例

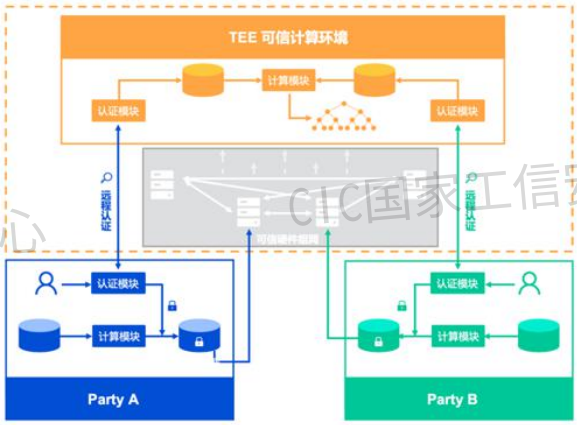

图 16 数据在 TEE 集群中的处理

来源：国家工业信息安全发展研究中心

上图描绘了一个典型的基于 TEE 的多方数据融合处理场景——多个参与方将加密数据传入 TEE 集群，并经过远程证明确认目标环境确实可信、且运行的是预期的可信应用，之后才允许数据在 TEE 中运算。此外，TEE 还可用于区块链链上隐私和链下隐私计算、面向机密数据的人工智能训练和预测、隐私保护的大数据处理、关键 IT 基础设施防护、安全可信的云计算等丰富的隐私计算场景。

机密计算结合多方安全计算等技术，可服务联合风控、智能营销等多个业务场景。例如，采用多方安全计算、可信执行环境双引擎的架构，并结合区块链、零知识证明、差分隐私等技术，可解决数据孤岛的隐私、共识、可信难题，满足客户不同的安全性和性能要求，解决区块链全生命隐私保护周期难题，应用于政企强隐私场景。基于机密计算构建的链下隐私计算平台，扩展区块链隐私及数据处理能力，将大数据、机器学习等引入区块链技

术生态，已规模化应用在数字物流、金融风控等领域。

五、可证去标识

可证去标识应用基于个人及参与方授权的数据输出，结果数据无法推断个人隐私或商业机密，保障数据挖掘过程中任何参与方无法接触用户隐私，但可参与数据价值挖掘。该技术通过创新的去标识技术和身份防关联技术，保证数据在分析和计算的过程中不会被关联到数据主体，并且只有获得授权的计算结果接收方才能恢复结果数据的主体信息。

（一）技术简介

可证去标识是一种面向大数据规模（百亿级）离线挖掘以及高性能实时决策（MS 级）场景、基于可证明去标识技术的多方隐私计算方案。主要特点是将隐私安全能力植入大数据计算、存储引擎等基础设施，构建一个大规模可信数据环境，各方数据在域内，提升多方数据融合计算过程中的隐私安全水位，实现数据融合计算过程中的可算不可识，且不改变业务原有技术栈和使用习惯，同时最小化改变数据内容，业务算法模型精度不折损。可信去标识和可证无身份关联等技术联合使用（称为隐私标识计算）可以一方面提供充分的隐私保护能力（符合 GB/T35273-2020《个人信息安全规范》和 JRT 0171-2020《个人金融信息保护技术规范》），另一方面保留数据原始颗粒度并支持高性能实时的计算和分析。

（二）技术优缺点

在数据规模较大（比如大于百万条记录）或对计算性能要求

较高时，基于多方安全计算或联邦学习的技术可能难以满足性能或者实时性需求。在大规模或实时性要求较强的数据分析场景下，可证去标识是目前唯一能同时满足隐私合规要求和计算性能要求的新技术。这种技术确保数据去标识后，数据接收方无法重新识别或者关联个人信息主体。可证去标识首先对参与计算的多方数据可信去标识管控，确保所有计算基于去标识化数据展开；其次构建集中式的可信计算环境，通过对试图关联或还原个体身份的高危行为进行拦截，实现挖掘过程中个人数据“可算不可识”；最后在结果输出阶段对输出数据进行原始数据拥有主体及用户的双重确权，实现了价值输出时各方权益可保障。该方案可与现有大数据技术栈无缝集成，且采用集中式计算规避了跨网延时成本，可支持大规模数据的高性能分析和计算，且计算场景受限较小，支持几乎所有类型的数据分析和建模，较好地平衡了个人隐私权保障、数据处理规模和业务实时性，适用于对计算环境存在信任基础的多方大规模数据挖掘场景。但可证去标识需明细个人属性数据需要流动，外部合作方可能存在信任障碍。

（三）国内主要厂商

1.蚂蚁集团

蚂蚁集团可证去标识适用于多方开展大规模离线数据挖掘以及高性能在线数据分析场景。可证去标识是一种全新的隐私计算技术，允许多方依法合规的使用数据，安全可控的进行数据分析和计算，同时支持大规模数据和实时计算。

（四）应用场景与案例

可证去标识适用于以下场景：一是快速拉升隐私安全及合规水位，例如 2 周完成微贷离线全域逻辑隔离及逻辑去标识，1 月完成贷后催收及关系网络物理链路整改。二是大规模数据挖掘及高性能实时决策，支撑搜索推荐百亿级数据处理及模型训练，首页推荐、大促会场等 200ms 内容推荐。三是融合数据可复用，支持常态化数据共享。

第三章 产业篇

现阶段尚未有精确的计算方法进行隐私计算产业规模的预测，但隐私计算在数据共享、流通、传输等方面均有涉及，结合我国大数据产业规模来看，隐私计算产品市场规模约为10亿，基于隐私计算的数据交易应用模式市场或将达到千亿级。

一、产业现状

从“十三五”期间的云计算、大数据、人工智能，到近年快速发展的区块链、物联网、量子计算，各界对数据安全性和隐私性的重视提高到了前所未有的高度，这都对数据安全及数据隐私保护都提出了更多更高的要求，隐私计算前景与市场潜力巨大。但产业目前处于初期探索阶段，从技术、企业主体、行业应用到市场模式仍有较大发展空间。

（一）技术层面，隐私计算多技术融合应用

通常隐私计算单一技术分支只在解决某特定问题上具有较好表现。因此在项目实践中，根据行业不同场景的信任假设以及需求的复杂性、多元性，需要选择整合多种技术的框架，以支持数据使用和可信计算的场景应用。具体而言，商业场景下的隐私数据保护是多元的，包括AI和非AI的需求、数据量区别、各方信任问题及保护对象的差异等，因此完备的数据处理的基础设施和系统不可能依赖单一技术。其中密码学作为严谨的技术基础，定义了系统安全阈值。在此基础上，所有安全技术都有性能损失，因此需要推动系统实现、技术组合以及密码技术迭代发展以提升

各项性能，城市级大型应用尤其如此。例如，湖北某市多点触发的传染病防控应用功能要求多样、数据来源广泛，涉及卫生健康、医院医药、公安、海关边防、教育、交通等各部门数据，在保密性、准确性和计算效率之间找到平衡点，体现了多技术融合的隐私安全计算应用价值，具体采用多方安全计算进行政务平台和健康医疗平台部分信息的联合查询和联合分析；采用联邦学习进行涉及多系统、多组织间的传染病疾控预警模型、症候群智能监控预警模型训练；此外采用区块链实现数据的链上存证核验、计算过程关键数据和环节的上链存证回溯，确保计算过程的可验证性等。

（二）主体层面，多方企业加码隐私计算

根据 Gartner 的预测，到 2025 年全球将有一半的大型企业机构在不受信任的环境和多方数据分析用例中使用隐私计算处理数据。近几年，大量专攻隐私计算的初创公司成立，致使自 2018 年起在隐私计算领域投入研究的企业数量激增。我国该领域的企业总量在 260 家左右，其中 2018 年至 2020 年的初创企业达 160 家，占比约为 60%。从企业行业分布来看，软件和信息技术服务业占比最高，约为 47%，此类企业包括专攻隐私计算技术领域企业及布局隐私计算领域的区块链、大数据厂商；商务服务约为 33%，此类企业主要围绕法律服务、咨询调查等提供中介服务；技术推广服务约为 13%，此类企业主要包括医疗、安防、人社等各领域的隐私计算应用企业；信息系统集成服务约为 7%，此类主要包括数据存储与处理、数据平台运营等数据服务集成商。

图 17 涉足隐私计算企业成立日期

来源：国家工业信息安全发展研究中心

从 2018 年开始，蚂蚁集团、百度、阿里、腾讯等互联网龙头企业，富数、同盾、星环等成熟的网络安全及大数据公司以及华控清交、锘崴科技等初创型科技企业，已接连入局隐私计算。此外，微众银行、平安集团等行业数据高度聚合企业涌入隐私计算领域，开展数据增值业务。

表 1 国内隐私计算厂商

厂商类型	厂商	核心技术/技术影响力	标杆案例
综合型互联网公司	蚂蚁	多方安全计算 MPC、联邦学习可信执行环境可信执行环境、差分隐私	浦发蚂蚁联合风控、跨医疗机构隐私计算平台网络（阿里云蚂蚁联合）、基于多方安全计算的在线健康险风控服务
	百度	参与国标制定(TC260, TC601, etc)、PaddleFL 框架开源， Meta 可信执行环境, BFC 通用安全计算平台	——
	腾讯	FL 应用服务白皮书，Gartner 在线反欺诈推荐厂商，安全竞赛名次	江苏银行、济宁银行、四川航空、腾讯医疗健康
	华为	联邦学习、多方安全计算、可信执行环境	探索初期，暂无
	字节跳动	开源两磅学习 FL 平台 Fedlearner FL 梯度保护算法	火山引擎（内部智科） 外部提升广告主投放效益
网络安全及大数据公司	京东数科	自研联邦学习 FL 平台	雄安新区“块数据平台”；南通新基建
	富数	多方安全计算/联邦学习	交通银行
	星环	联邦学习	电力数据看经济
	同盾	联邦学习	合作银行
金融机构	平安科技	蜂巢联邦学习智能平台, IDC 奖项	金融子公司联合建模，精准获客

	微众银行	联邦学习 C 位, FATE 开源, FL 白皮书 2.0,大量 FL 行标	极视角“视觉联邦系统"、一嗨租车、山东高速金服，同济大学药物隐私
初创专精型公司	翼方健数	安全沙箱、联邦学习	厦门健康医疗大数据平台
	华控清交	多方安全计算	基于多方安全计算的人脸识别验证数据安全融合平台、云上贵州数据安全可控开发利用云平台
	数牍	多方安全计算	联通大数据公司数据科学研发平台建设中国移动多方支全计算平台(试点)
	蓝象	多方安全计算	——
	锘崴	联邦学习	基因检测

来源：国家工业信息安全发展研究中心

但隐私计算从单一技术到场景落地面临诸多挑战，落地效果取决于厂商的多方面能力，包括产品、技术、实施与服务、生态建设等。市场发展初期，行业标准尚未完全建立，大批技术水平参差不齐的厂商进入，市场鱼龙混杂。第一梯队企业已建立开源社区、开放平台、隐私计算相关产业联盟，着力构建隐私计算生态体系，打造数据经济体。第二梯队企业自主开发隐私计算技术，已在行业形成丰富的应用实践，累计大量特定场景的数据模型。但大量企业基于 tensorflow 等开源工具构架隐私计算能力，研发水平不足。

（三）应用层面，金融及医疗行业应用发展最快

获取用户数据涉及科技型企业的核心竞争力，收集大量个人数据实现了用极低的边际效应实现新的产品，例如在互联网公司的收益中占比极高的广告投放。这是隐私计算前景及需求较高，但目前除互联网领域外，仅在金融、医疗（如下图）等强监管领域有较多实践的原因。

图 18 隐私计算图谱

来源：国家工业信息安全发展研究中心

医疗数据是个人隐私的最后防线，自身具有高价值与隐私性强等特点，其使用权与所有权的矛盾始终存在。而隐私计算的出现化解了这一矛盾进而在医疗领域前景广阔，呈现自上而下、自下而上双向并行的现象。国家层面，国家医疗健康大数据首批试点城市厦门构建了基于隐私安全计算技术的“健康医疗数据应用开放平台”，在保证数据隐私的前提下，通过开放平台提高数据使用效率，打破数据孤岛，构建了一个医疗数据应用开放的数据生态。企业层面，隐私计算技术厂商积极对接医疗大数据国家队为合作对象，例如翼方健数搭建城市医疗信息平台，依托城市医疗数据发展医疗领域隐私计算；锘崴科技瞄准基因数据库，研究隐私计算在基因组数据联合共享和分析过程中的应用。

金融行业落地条件成熟，是隐私计算的最佳切入点。一是金融行业存在较多数据交易，由于监管趋严，对隐私计算的需求增强；二是金融行业的客户付费能力强，商业模式变现空间大；三是金融行业数据基础设施完善，对数据安全的要求也最为严格，因此金融领域应用案例向其他行业推广的复制性强、可用性广。目前，隐私计算在金融领域主要有以下几方面：最大的应用体现在风控模型联合建模上，在银行、互联网金融、消费金融等机构得到广泛应用；其次，保险等金融机构运用隐私求交等隐私计算技术联合外部数据合作方建立精准的营销模型；此外，信贷业务企业在名单共享、多头借贷信息共享等方面使用隐私计算在反欺诈中保护隐私及商业秘密。

（四）市场层面，尚未形成成熟的市场环境及商业模式

隐私计算的市场环境及商业模式尚未成熟。市场环境方面，由于隐私计算技术复杂且常常呈现“黑盒化”现象，且处理对象常涉及敏感数据资产，隐私计算众多技术提供方须首先建立信任，提升需求方接受程度。长期来看，隐私计算有可能从合规避险的技术手段上升为数据产业链的重要环节。但目前隐私计算效率问题、框架可操作性等问题仍需解决或进一步改善，现象级的跨越发展需要明确的政策拉动等契机催动。

从商业模式分析，数据资源型企业将向平台型企业发展，更加注重与上游数据源企业的对接，积累高价值数据源合作方，并从数据质量测试等方面入手保障数据可用性。技术创新型企业将深耕某场景解决方案，注重提升对技术需求方的服务能力，针对

个性化、多元化的需求快速私有化部署软硬件，保障各项性能指标满足需求方吞吐量、延时性等实际要求。两类企业将在较长时间维持共生甚至合作关系，尤其目前隐私计算前期验证阶段，行业较长时间内定制化需求较高，且市场处于对隐私计算技术提供机构的信任构建期，中立厂商大有可为，将形成“多山头”局面。

二、产业环境

Gartner 将隐私计算作为 2021 年重要战略科技趋势。隐私计算已成为近两年的热点，并将在接下来的几年持续保持热度。现阶段，产业已涌现出一批创业型企业，该领域也成为投融资机构的关注焦点之一。此外，随着创新成果的转化，相关技术专利申请与标准化建设也在持续推进。

（一）政策支持：多部门多地发布规划支持隐私计算

我国以政策手段促进技术创新发展，利用规划指明发展方向，防止监管遏制科技进步。在数字经济迅速发展的背景下，隐私计算技术的关键作用正在逐渐显现，发展规划等各项相关推进政策也将不断向行业化、地方化方向细分发展，自 2019 年起多行业各地方规划提出研究利用隐私计算解决相关问题（如下表）。从行业角度来看，近两年隐私计算政策侧重于金融科技、工业大数据、区块链三个领域。在地方层面，2020 年，湖南、山东、上海等地区都对隐私计算做出了更为细致的规划。可以肯定的是，在未来 5 年时间，我国关于隐私计算的相关政策和立法的落实、执行及深化将进一步推动行业发展需求。除了个人数据及隐私保护，国家在数据安全、数据要素流通等方面的一系列举措，更将从数据监

管和国家利益的高度确立隐私计算的巨大价值和重要地位。

表 2 明确发展隐私计算的政策文件

政策名称	地区	发布时间
《金融科技（FinTech）发展规划（2019-2021 年）》	国家（人民银行）	2019.8.26
《工业大数据发展指导意见（征求意见稿）》	国家（工信部）	2019.9.4
《关于加快构建全国一体化大数据中心协同创新体系的指导意见》	国家（国家发改委）	2020.12.23
《湖南省区块链发展总体规划（2020 — 2025 年）》	湖南省	2020.10.27
《关于印发山东省推进工业大数据发展的实施方案（2020-2022 年）的通知》	山东省	2020.12.9
《赣州市数字经济发展规划（2019-2023 年）》	江西省赣州市	2020.3.10
《贵阳贵安区块链发展三年行动计划（2020-2022）》	贵州省贵阳市	2020.7.3
《广西壮族自治区区块链产业与应用数据发展规划（2020—2025 年）》	广西省	2020.8.6
《杭州国际金融科技中心建设专项规划》	浙江省杭州市	2020.7.17
《上海市公共数据开放管理办法（草案）》	上海市	2019.4.29
《湖州市人民政府关于印发湖州市公共数据安全管理暂行办法的通知》	浙江省湖州市	2020.12.23
《成都市金融科技发展规划（2020-2022 年）》	四川省成都市	2020.5.9

来源：国家工业信息安全发展研究中心

（二）金融保障：隐私计算领域投融资以 Pre-A 轮为主

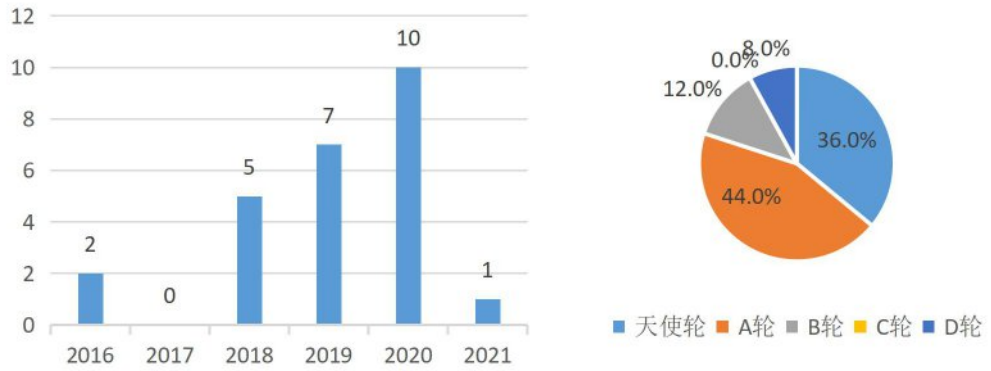

图 19 年度隐私计算融资事件数量及隐私计算融资轮次分布

来源：国家工业信息安全发展研究中心

自 2016 年起，隐私计算领域融资 28 起。随着资本关注度的提升，融资事件基本呈现逐年递增的情况。从融资事件来看，微众银行及矩阵元于 2016 年最早获得 A 轮投资。微众银行、翼方健数、数篷科技、趣链科技、DataExa、星环科技、京东数科、同盾

科技融资金额超 1 亿人民币。其中融资金额最高达到 17.8 亿人民币。从融资轮次来看，92%的融资事件处于 B 轮及 B 轮之前，其中天使轮及 A 轮占比达到 80%。

隐私计算目前处于起步阶段，大多数企业组建小规模团队内部试验或初步形成产品，尚未形成成熟的商业模式，因此融资基本集中在 B 轮之前。对于投资机构而言，现阶段重点关注隐私计算企业的核心技术竞争力及团队优势。

（三）专利申请：隐私计算近两年内专利申请量激增

图 20 年度隐私计算专利申请量

来源：国家工业信息安全发展研究中心

自 2017 年起，专利申请量飞速上升，截至 2021 年 4 月，隐私计算相关专利近 5000 项。**从专利领域来看，**隐私计算研究热点主要集中在协议，软件平台的访问控制，利用校验、证书和签名保障数据完整性，密钥分配，系统用户身份或凭据检验等方面。**从机构数量上看，**目前隐私计算申请机构第一序列中企业与高校参半，企业创新主体地位不明显，仍有相当数量的技术创新成果

由高校主导。但深度布局隐私计算的企业投入大量研发人员力量，专利申请量总数超过各高校。例如，蚂蚁集团、微众银行隐私计算研发团队达到 500 人，阿里巴巴相关人员达到 200 人，矩阵元及平安科技的团队规模也在 100 人左右，5 家企业共申请专利近 1000 项，约占专利总量 20%。此外，隐私计算头部企业在人员配置比例中加大算法及密码学人员数量，并注重以隐私计算领域专家培养团队。

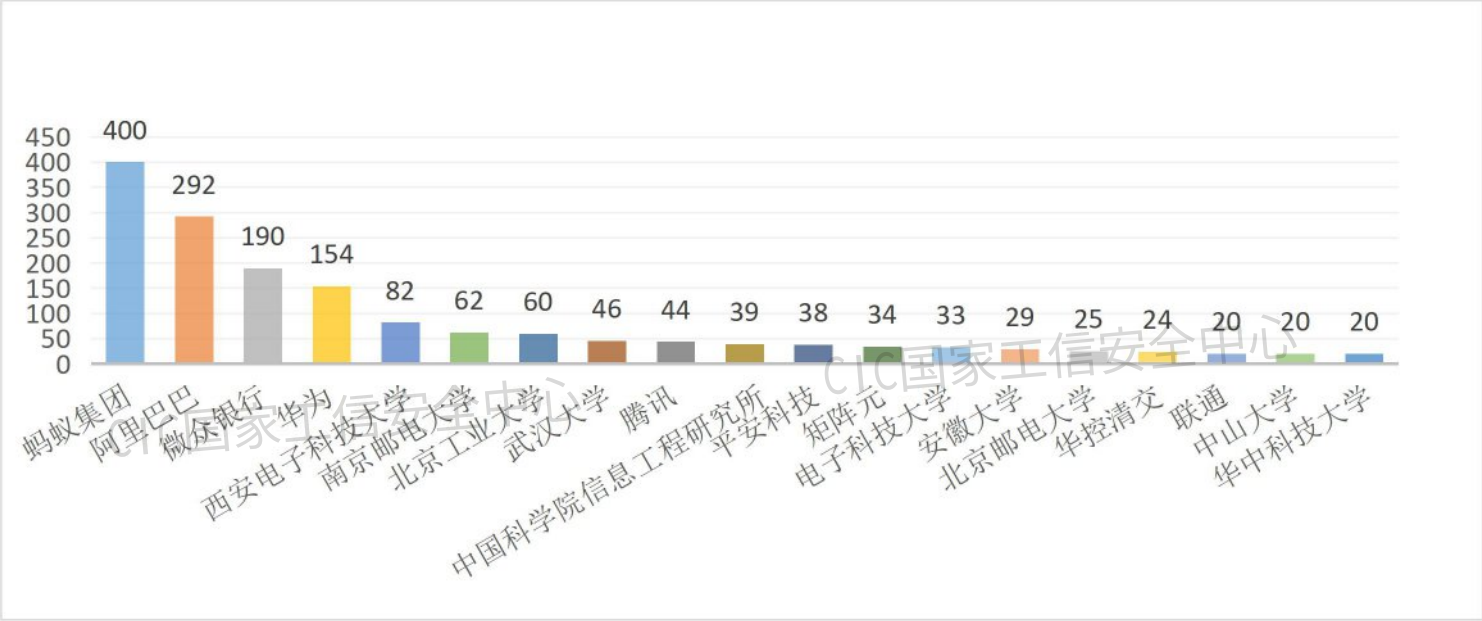

图 21 各机构专利申请数量

来源：国家工业信息安全发展研究中心

随着企业将各项研究成果全面应用于产品，较长时间内隐私计算领军企业仍将在专利方面聚焦发力，以尽快形成一批产业化导向的关键技术专利组合，并逐步形成完整的隐私计算技术布局；此外，微众银行等领军企业逐步开源隐私计算框架，也将方便高校进一步研究。未来几年隐私计算领域专利将以较高增长率持续上升。

（四）标准建设：国内外标准化组织均已开展研制工作

目前，金标委、信安标委、中国通信标准化协会、IEEE、ITU-T、ISO 等各个标准化组织，针对数据共享流通应用的技术如联邦学习、多方安全计算、可信执行环境等各个技术领域，已经开展了相关领域的技术标准研制工作。国际标准方面，ISO/IEC JTC1 的 SC27 信息安全分技术委员会在隐私框架方面已经制定了诸多标准，如隐私框架与架构（ISO/IEC 29100、ISO/IEC 29101）等，该部分标准是隐私计算的隐私保护基础标准。此外，IEEE 也于 2019 年开始了多方安全计算、共享学习的国际标准制定工作，并陆续开展了基于可信执行环境的安全计算、联邦学习技术框架与应用指南等标准制定工作。国际电信联盟标准化部 ITU-T 分别在 SG16 和 SG17 开始制定共享学习和多方安全计算的国际标准。国家标准方面，目前针对多方安全计算、可信执行环境、联邦学习已有 3 项测试标准，此外另有联邦学习参考框架、基础架构与应用两项团体标准。

标准化工作需要科学的顶层设计，隐私计算等软件和信息技术类标准通常从基础支撑、技术方向、产品工具、规范管理及行业应用等方面构建高质量、体系化的标准体系（如下图）。总体而言，我国隐私计算领域现有标准从隐私计算技术类型及标准内容方面缺乏大量针对性的专用标准，尚未形成具有指导作用的标准体系，需要通过标准化的途径规范认知，促成行业共识，推进隐私计算产业健康发展。2021 年 3 月，工信部发布的年度标准工作要点，明确提出将围绕包括网络和数据安全在内的安全生产领域编制强制性国家标准体系建设指南。随着隐私计算技术发展、应

用落地、监管收紧，标准化建设工作需求将越来越迫切。下一步，隐私计算标准化工作将集中以下方面：一是促进不同厂商及技术之间互联互通；二是各细分场景的隐私计算安全分级，例如原始数据的计算性和隐私性、计算过程的安全性、结果信息反推原始数据的安全性等。

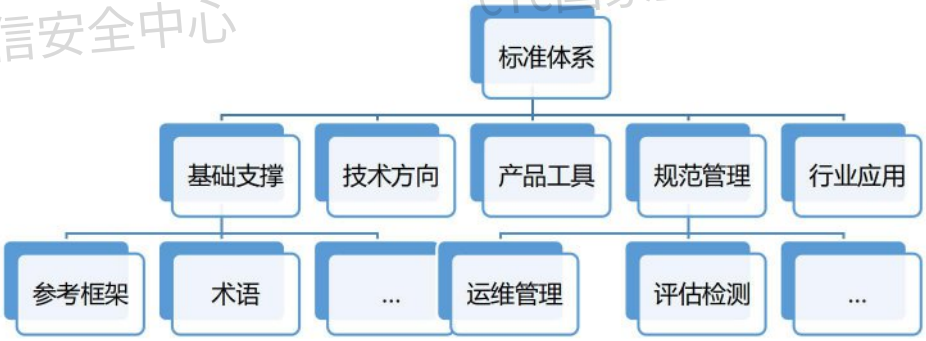

图 22 软件和信息技术类标准体系

来源：国家工业信息安全发展研究中心

第四章 建议篇

一、健全法律法规明确隐私计算发展方向

一是建立健全数据安全保护相关法律法规，完善隐私计算技术应用顶层设计。现有法律法规未对多方安全计算、联邦学习等等隐私计算技术的应用条件、范围等进行明确界定，导致技术需求方及社会大众对相关技术应用方的信任度不足，部分行业推广较为困难。例如，个人信息用于隐私计算是否属于数据安全法例外条款，目前并无明确规定。因此，需通过数据安全领域立法对隐私计算技术应用的合法性与合规性作出合理界定，鼓励新技术为数据安全领域提供解决方案，为隐私计算技术的发展指明方向。

二是平衡好技术推广应用与数据安全保护关系。一方面，隐私计算立法需要为数据要素市场化配置保留空间，鼓励新技术的推广应用。例如，隐私计算立法若要求数据经过严格的匿名化才能融合共享或不区分场景地要求用户授权，则将大大削弱数据要素价值或者导致数据价值不可利用。另一方面，隐私计算立法的出发点和落脚点是加强数据安全保护，因此需在司法实践中检验检测技术的应用效果，加强监管以防止技术滥用。这些问题需要法律界和工业界共同努力，在隐私计算技术推广应用与数据安全保护中找到最佳平衡点。

二、构建标准体系提供隐私计算应用规范

一是通过国家标准、行业标准等进一步规范隐私计算落地应用。隐私计算技术目前尚处在发展初期，但行业中百花齐放的发

展格局已初见端倪，亟待相关企业、协会及科研院所建立标准体系，规范技术应用并形成行业共识。标准体系应明确界定隐私计算技术的相关定义，并对隐私计算的应用范围、技术指标等提出量化要求，从而规范隐私计算技术供给企业的研发与经营，提升技术安全性。

二是建立隐私计算应用测试评估标准体系。在隐私计算技术发展期及膨胀期，市场中也极易出现解决方案的数据保护水平高低不均、落地效果良莠不齐的现象。因此，需制定面向隐私计算技术应用的测试评估标准，在市场端对技术落地应用进行质量监管。通过具有资质的国家级、行业级第三方评估机构对隐私计算技术应用效果及安全性进行检验检测，从而提升隐私计算需求企业及公众对技术的信任度，保障隐私计算产业应用的健康发展。

三、培育数据要素市场完善产业发展环境

一是进一步促进数据流通，扩大隐私计算应用场景。安全性是数据资源在数据要素市场释放价值的重要保障，数据要素市场对隐私计算技术具有显著需求，并为其提供了广阔的应用环境。目前，我国数据要素市场高附加值业务仍沿用传统渠道流通数据源，数据交易及产品定价模式尚需探索。因此，我国数据要素市场应进一步促进数据交易流通，盘活数据资源，为隐私计算技术提供更多应用场景。同时，隐私计算技术也将在市场机制作用下不断创新，实现技术迭代与研发突破。

二是培育更加完善的数据要素市场，提升数据质量。由于隐私计算算法敏感度较高，且多用于跨企业甚至跨行业的数据流通，

对参与方的数据规范性、一致性以及数据质量要求也较高。当前大部分企业的数据规范性和质量难以支撑隐私计算技术，因此应培育更多数据要素市场合格主体，进一步提升数据要素市场整体数据质量，为隐私计算技术大规模应用创造先决条件。