CAICT 中国信通院 阿里安全 ALIBABA SECURITY 数牍科技 SUDO PRIVACY

隐私保护计算技术研究报告

（2020 年）

中国信息通信研究院安全研究所
阿里巴巴集团安全部
北京数牍科技有限公司

2020 年 11 月

版权声明

本报告版权属于中国信息通信研究院、阿里巴巴（中国）有限公司以及北京数牍科技有限公司，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国信息通信研究院、阿里巴巴（中国）有限公司、北京数牍科技有限公司”。违反上述声明者，编者将追究其相关法律责任。

前　言

2020 年 6 月，世界银行发布的《全球经济展望》预计[1]，2020 年全球经济将收缩达 5.2%，由新冠肺炎疫情引发的全球经济衰退将成为第二次世界大战以来程度最深的衰退。叠加全球疫情发展的不确定性及逆全球化趋势逐渐显现等多重困境，各国经济发展面临着严峻的挑战。

“百舸争流，奋楫者先”[2]。面对错综复杂的世界经济格局，数字经济凭借其坚强的韧性和巨大的潜力，实现了经济逆势增长。为了抢抓数字经济快速发展的历史机遇、赢得全球数字经济博弈主动权，世界各国均将发展数字经济作为经济复苏的关键举措。2020 年 9 月，新美国安全中心（Center for a New American Security，CNAS）发布了《设计美国数字发展战略》，确定了促进美国数字发展战略全面、协调发展的四项指导原则，明确了美国政府、私营部门在美国数字战略发展中的地位和作用，以及对国际竞合关系的战略定位，同时就国际技术合作、标准制订、人才队伍建设等方面提出五大建议，为制定具有竞争力的美国数字发展战略提供了依据。欧盟积极布局人工智能领域，先后制订《欧洲人工智能协调计划》《可信赖人工智能的道德准则草案》《人工智能白皮书》等，力争在人工智能伦理规范制订层面发挥引领作用。我国则把培育数据要素市场作为发展数字经济的重点，先后发布《中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定》《中共中央

[1] World Bank Group: Global Economic Prospects.
[2] 《礼记. 中庸》

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》等相关文件，要求加快培育数据要素市场，提升数据要素价值。

“上下求索，吹沙见金”[3]。数据的价值从数据源挖掘而出，是“被动产生的”，具备哲学领域的“第二性”。静态的孤立数据是没有价值的，数据要素流转才能实现数据价值挖掘，为探索客观世界新规律、降低决策过程的主观影响提供可能，深刻赋能数字经济。人类社会欲实现享受数据价值红利的愿景，在拥抱数据价值之前，更加需要明确数据流通与协作过程所面临的风险与阻碍。如何在保证数据安全的前提下，实现数据的协同应用成为充分释放数据价值的关键。隐私保护计算作为保障数据价值挖掘过程中隐私安全的关键技术，在金融、政务、医疗等行业应用中赢得了光明的市场前景。

“知所从来，思所将往”。本报告详细介绍了隐私保护计算的概念内涵，提出了隐私保护计算的保护目标，深刻探讨了数据流通与协作过程中面临的“数据孤岛”、合规趋严和信任鸿沟等问题，详细分析并对比了联邦学习、安全多方计算、机密计算、差分隐私、同态加密等关键隐私保护计算技术，介绍了隐私保护计算在金融、政务、医疗等领域的部署经验，并对隐私保护计算未来发展进行了展望，以期为关注隐私保护前提下的数据要素市场培育、国家网络安全实力综合提升的社会各界提供有益借鉴与参考。同时，针对报告中的诸多不足，恳请各界同仁批评指正。

“建久安之势，成长治之业”[4]。在数字经济发展的大背景下，

[3] 《中国制度面对面——理论热点面对面·2020》，学习出版社、人民出版社。
[4] 《汉书. 贾谊传》

我们深知数据安全及隐私保护有着丰富的内涵和广泛的外延，不仅包含法律的修缮，还包含安全技术的迭代升级等诸多方面。如何在保障数据隐私安全的前提下，加快培育数据要素市场，亟待多方共同协作努力。在日渐激烈的数字博弈背景下，我们始终坚信“道阻且长，行则将至；行而不辍，未来可期。”

本报告的编制过程中，得到了来自阿里巴巴集团安全部，北京数牍科技有限公司的大力支持。借此，谨向支持本报告编制工作的各位领导以及付出辛苦劳动的编制人员表示感谢。

CAICT 中国信通院

目 录

一、隐私保护计算.....6
（一）隐私保护计算概念.....6
（二）隐私保护计算架构.....6
（三）隐私保护计算目标.....7
（四）隐私保护计算价值.....8
二、隐私保护计算关键技术.....10
（一）联邦学习.....10
（二）安全多方计算.....17
（三）机密计算.....29
（四）差分隐私.....35
（五）同态加密.....38
三、隐私保护计算关键技术综合评价.....40
四、隐私保护计算应用案例.....44
（一）金融领域.....44
（二）政务领域.....45
（三）医疗领域.....46
五、 隐私保护计算发展展望.....48

CAICT 中国信通院

图 目 录

图 1　隐私保护计算参考架构.....7
图 2　面向数据生命周期的隐私计算技术.....8
图 3　基于联邦学习的语言预测模型更新.....11
图 4　横向联邦学习.....13
图 5　纵向联邦学习.....13
图 6　联邦迁移学习.....14
图 7　联邦学习参考架构.....14
图 8　安全多方计算示意图.....18
图 9　2 取 1 不经意传输协议.....22
图 10　AND 门混淆电路示意图.....23
图 11　安全多方计算参考架构.....24
图 12　Intel SGX 基本原理.....31
图 13　Rust SGX 架构示意图 [30].....33
图 14　消息传递接口示意图.....34
图 15　反欺诈联邦学习示意图.....45
图 16　疑犯信息查询示意图.....46
图 17　新冠人工智能联合诊断示意图.....48

表 目 录

表 1　通用安全多方计算实施方案对比.....27
表 2　关键技术综合评价表.....43

CAICT 中国信通院

隐私保护计算技术研究报告

2019 年 10 月，党的十九届四中全会决议通过的《中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体系和治理能力现代化若干重大问题的决定》（以下简称《决定》），首次增列“数据”为生产要素，要求健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制。纵观社会经济发展，从以土地、劳动力为生产要素的农业经济时代，到以资本、技术为生产要素的工业经济时代，演进至今以数据生产要素为核心推动力的数字经济时代，生产要素形态的演进具有鲜明的社会经济发展时代特征。随着经济的发展和进步，由于自然资源的不可再生性、人口红利逐渐弱化、技术贡献逐渐乏力等因素导致传统生产要素对经济增长的拉动作用逐渐减弱，全要素生产率增长乏力。而数据要素打破了原有自然资源的有限性，实现可复制、可共享，为经济持续增长释放了无限的潜能。将数据增列为生产要素，是对数据生产价值、市场贡献以及历史地位的高度肯定。

为落实党的十九届四中全会关于《决定》的重大决策部署，2020 年 4 月，中共中央、国务院出台《关于构建更加完善的要素市场化配置体制机制的意见》（以下简称《意见》）。作为我国首份要素市场化配置的文件，《意见》围绕数据生产要素，强调从**推进政府数据开放共享、提升社会数据资源价值、加强数据资源整合和安全保护**三方面加快培育数据要素市场。《意见》对数据生产要素市场培育的理论创新和方法论指导，对于全面释放数字红利、助推国家抢抓数字经济

全球竞争制高点具有重大战略意义。

由希捷公司资助，IDC 发布的《数据时代 2025》白皮书显示（2020 年 5 月数据更新），相较于欧洲、中东、非洲、美国、亚太（含日本，不含中国）以及全球其他区域，在未来 5 年我国的数据量年平均增长率将达到 26%，预计到 2022 年将拥有全球最大的数据圈（datasphere）[5]。如何加快培育数据要素市场成型，激发数据要素市场活力，充分发挥数据生产要素对其他要素的倍增作用，亟待多方协同努力开拓。数据要素的流通共享和核心价值挖掘是数据要素市场培育的核心内容，必须在保证隐私安全的前提下实现有效信息共享，在兼顾其它生产要素实现资源统筹优化、提高资源配置效率的同时，反哺农业经济和工业经济，实现资源配置最优组合服务社会，孕育更大的数据价值，为数字经济繁荣创造条件。从当下数据流通的实践来看，传统基于所有权转让的交易模式仍然受困于交易形态、数据确权、数据定价等问题而无法规模化落地，依托于隐私保护计算的数据协同应用平台的服务模式更为可行。当前，仍然有三大因素制约数据流通与协作。**一是**“数据孤岛”现象普遍存在；**二是**全球数据合规监管日趋严格；**三是**隐私泄露事件频发导致信任鸿沟。

“数据孤岛”现象普遍存在。随着信息化、智能化进程的不断推进，“数据孤岛”作为一个全球性问题已成为制约数据核心价值挖掘的瓶颈之一。“数据孤岛”的产生与企业的集团化发展模式和信息化的“需求优先”建设思路有着必然的联系，各子公司、各部门的数据

[5] IDC: Data Age 2025The Digitization of the World From Edge to Core.

形成彼此相互“独立”无法互通关联的一座座“孤岛”。“数据孤岛”的独立性不仅仅体现在物理数据存储和维护方面，更体现在企业间、部门间由于业务背景不同造成对数据的定义和使用差异化的逻辑性方面。“数据孤岛”的出现使得数据共享和流通协作受阻，无法保证数据的一致性和准确性，对于数据的核心价值挖掘造成了一定的阻碍。此外，由于数据要素的低成本可复制性，使其具有明显的规模经济效应，导致数据要素在资产化过程中极易发生垄断。**如何打破产业链上下游既有的数据壁垒，有效解决数字市场的竞争与垄断问题，充分激发数据要素价值、共享数字红利，实现数字经济时代的“耕者有其田”，已然成为社会各界关注的焦点。**

全球合规监管日趋严格。2018 年 5 月 25 日，欧盟《通用数据保护条例》（General Data Protection Regulation, GDPR）正式生效。为充分实现个人数据安全，GDPR 围绕个人数据处理行为组织者的义务主体和个人数据权利主体两方面搭建个人数据保护框架。此外，GDPR 也凭借其极高的域外适用效力，被称为史上“最严格”的数据保护管理条例备受全球关注。GDPR 的实施不仅向世界宣示了欧盟肩负重建数字经济时代隐私保护新秩序的雄心和决心，对世界各国关于隐私保护监管框架的构建与升级产生了深远的影响，也预示着隐私问题已切实成为悬在头上的“达摩克利斯之剑”。在 GDPR 正式生效一个月后，美国加利福尼亚州颁布了《2018 加利福尼亚州消费者隐私法》（California Consumer Privacy Act of 2018，CCPA），并于 2020 年 1 月 1 日正式实施。相较于 GDPR，CCPA 在倡导对个人数据隐私

被动防御和主动实施方面有着极大的相似性。但在个人信息概念界定、个人信息主体权利的丰富程度、个体意愿表达、出于利益平衡的数据合理应用等方面都体现出了较大的差异性。如 CCPA 对个人信息的收集使用采取“默示同意”（opt-out）模式，而非 GDPR 的“明示同意”（opt-in）模式。2020 年 6 月 28 日，第十三届全国人大常委会第二十次会议初次审议了《中华人民共和国数据安全法（草案）》（以下简称《数据安全法（草案）》）。《数据安全法（草案）》贯彻落实总体国家安全观，确立了数据安全保护的各项基本制度，坚持安全与发展并重，鼓励与促进数据依法合规的有效利用，促进以数据为关键生产要素的数字经济发展。2020 年 10 月 21 日，《中华人民共和国个人信息保护法（草案）》（以下简称《个人信息保护法（草案）》）公布并公开征求社会公众意见。《个人信息保护法（草案）》围绕总则、个人信息处理规则、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人信息处理者的义务、履行个人信息保护职责的部门、法律责任和附则等多个层面设计和建构个人信息保护的立法框架。**日趋严格的隐私保护监管一方面促进了数据权利主体和数据处理行为组织者的隐私保护意识的觉醒，但同时也加重了企业对数据流通与协作合法合规的担忧。**

隐私泄露事件频发导致信任鸿沟。2017 年，英国期刊《经济学人》（《The Economist》）发表封面文章称数据已经取代“石油”[6]成为当今世界最有价值的资源，将数据的重要性提到了无与伦比的高度。

[6] The Economist: Regulating the Internet Giants-The World’s Most Valuable Resource Is No Longer Oil, But Data.

基于对数据经济价值的高度认可，以及快速实现商业变现的盲目追逐，缺乏隐私保护的数据“野蛮掘金”活动日益猖獗，对于个人隐私的侵犯无处不在。2018 年 3 月，数据分析公司剑桥分析（Cambridge Analytica）被爆违规窃取 Facebook 用户数据并将之不当应用于政治广告投放和大选营销，实现了以经济利益为根本的政治目的。“剑桥分析”事件后，美国联邦贸易委员会（Federal Trade Commission，FTC）重启了对 Facebook 是否违反“2012 和解令”的调查，而 Facebook 也因未采取充分的隐私保护机制，与美国联邦贸易委员会达成彼时罚金最高的 50 亿美元和解协议[7]。随着万物互联愿景的逐步实现，数据作为人类与设备间的桥梁作用逐步显现，数据间的关联程度日渐增强，单点数据泄露事件的发生，极易被级联放大，足以引起一场“多米诺骨牌”效应的连锁危机。**在隐私意识逐步觉醒和合规监管日趋严格的大背景下，频发的隐私泄露事件进一步打击了社会各界对数据流通与协作的隐私保护信心。**

数据价值挖掘和隐私保护并非一场零和博弈，它们有着促进数字经济发展的共同理想和合作共赢的利益诉求。片面的共享集中及不切实际的隐私期待极易使得数据价值挖掘陷入“囚徒困境”。如何打破“数据孤岛”壁垒，建立数据流通与协作的隐私保护信心，以更加弹性柔软的方式促进法律监管“硬制度”的“软着陆”，实现数据价值挖掘和隐私保护的正和博弈，**隐私保护计算**为此提供了行之有效的解决之道。

[7] FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

一、隐私保护计算

（一）隐私保护计算概念

隐私保护计算(**Privacy-Preserving Computation**)近年来被提出，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[8]。面对数据计算的参与方或其他意图窃取信息的攻击者，隐私保护计算技术能够实现数据处于加密状态或非透明（Opaque）状态下的计算，以达到各参与方隐私保护的目的[8]。隐私保护计算并不是一种单一的技术，它是一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系。隐私保护计算能够保证满足数据隐私安全的基础上，实现数据“价值”和“知识”的流动与共享，真正做到“数据可用不可见”。

（二）隐私保护计算架构

隐私保护计算架构可抽象为图 1。在隐私保护计算参考架构中，主要有**数据方**、**计算方**和**结果方**三类角色。**数据方**是指为执行隐私保护计算过程提供数据的组织或个人；**计算方**是指为执行隐私保护计算过程提供算力的组织或个人；**结果方**是指接收隐私保护计算结果的组织或个人。为实现数据资源的丰富、升维以及模型的智能化应用，在实际部署中参与实体至少为 2 个，每个参与实体可以承担数据方、计算方和结果方中的一个或多个角色。例如在 P2P 的对等网络架构中，数据方同时承担了计算方和结果方的角色。

[8] UN Handbook on Privacy-Preserving Computation Techniques.

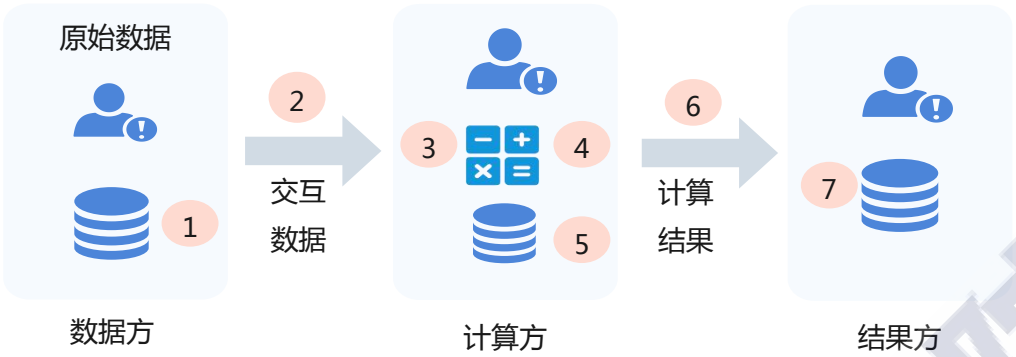


图 1　隐私保护计算参考架构

（三）隐私保护计算目标

根据图 1，隐私保护计算过程中主要存在 7 个隐私风险点[8]:

1) 数据在数据方的静态存储风险;

2) 数据从数据方传输至计算方的传输风险;

3) 数据在计算方**计算时的隐私风险;**

4) 数据在计算方**计算后的隐私风险;**

5) 计算结果在计算方的静态存储风险;

6) 计算结果从计算方传输至结果方的传输风险;

7) 计算结果在结果方的静态存储风险。

数据隐私计算技术广义上来说是面向隐私信息全生命周期的隐私保护计算理论和方法[9]。但在数据传输和数据存储环节的隐私保护技术已相对成熟，如 SM2、SM3、SM4、RSA、SHA2、AES 以及 SSL/TLS 等（如图 2 所示）。**故本报告提出的隐私保护计算则重点关注数据计算过程和数据计算结果的隐私安全问题。**

[9] 李凤华，李晖，贾焰, 等. 隐私计算研究范畴及发展趋势[J]. 通信学报，2016，37(04):1-11.



图 2　面向数据生命周期的隐私计算技术

隐私保护计算的目标是在完成计算任务的基础上，实现**数据计算过程**和**数据计算结果**的隐私保护。**数据计算过程的隐私保护指参与方在整个计算的过程中难以得到除计算结果之外的额外信息。数据计算结果的隐私保护指参与方难以基于计算结果逆推原始输入数据和隐私信息。**

（四）隐私保护计算价值

在消除“数据孤岛”方面。“数据孤岛”的出现是企业集团化发展和信息化进程的“必然产物”，但是越来越多的企业和组织需要与产业上下游的业务伙伴通过数据流通实现深度合作，以此来提升决策能力，获取竞争优势。物理和逻辑上的孤立性叠加日渐趋严的合规监管和隐私保护意识的觉醒，使得数据价值释放举步维艰。而以联邦学习、安全多方计算、机密计算、差分隐私、同态加密等为代表的隐私保护计算从技术角度实现了原始数据不出库、数据“价值”和“知识”出库的目标，有效实现跨领域多维度数据的融合，完成了数据流通向“价值”流通的升级，打破既有数据壁垒，有效实现了数据隐私保护

与价值挖掘之间的平衡，构建了一种“数据可用不可见”的合作新模式。

在合规避险方面。欧盟的数据市场报告显示[10]，2019 年欧盟 27 国及英国的数据经济价值已经突破 4000 亿欧元（4064.68 亿欧元），年增长率达 7.6%，预计 2020 年达 4439.25 亿欧元，预计年增长率达 9.2%，数据经济对欧盟 2019 年 GDP 贡献比已达 2.6%。在数据隐私保护合规监管日趋严格的大背景下，欧洲数据经济相当程度的规模化和商业化发展一定程度上实现了 GDPR 开宗明义所传承的二元立法目标：保护个人权利并促进个人数据流动。这与欧洲在隐私保护计算技术合规性研究方面做出的巨大努力密切相关。其中关于隐私保护计算技术的一个重要范例是爱沙尼亚在 2015 年的私人统计项目，1000 万条可识别纳税记录与 60 万条可识别学历信息关联在一起，通过安全多方计算技术对其进行统计分析。欧洲的 PRACTICE 项目（欧盟第七框架计划）付出大量努力分析安全计算技术的合规性[8]，报告依据 GDPR 论证了该爱沙尼亚项目的合规性，为欧洲实现隐私保护合规的高效数据流通提供了重要范例。

在弥合“信任鸿沟”方面。数字经济时代，我们一方面高度认可数据所蕴含的巨大价值，但另一方面频发的隐私泄露事件也引发了公众对数字经济发展中的隐私保护能力的信任危机。对待数字经济时代的数据价值挖掘，我们应该始终坚持包容审慎的态度，积极探索隐私保护和数据价值挖掘的平衡点。如何弥合数字经济时代的信任鸿沟，

[10] The European Data Market Monitoring Tool.

有效规避隐私侵害，隐私保护计算对于破解公众的信任危机是显而易见的。以安全多方计算、差分隐私、同态加密等为代表的隐私保护计算技术凭借其坚实的理论基础和安全性证明，从技术角度实现数据主体权利和数据使用者义务的平衡，增强数据应用透明度，提升了数据价值挖掘下的隐私保护信任，对于弥合数字经济时代的信任鸿沟具有重大意义。

二、隐私保护计算关键技术

隐私保护计算（Privacy-Preserving Computation）的概念虽然是近年来才被提出，但其涵盖的技术理论研究却有着相当的历史。总体来说，隐私保护计算技术通常涵盖联邦学习、安全多方计算、机密计算、差分隐私、同态加密等。

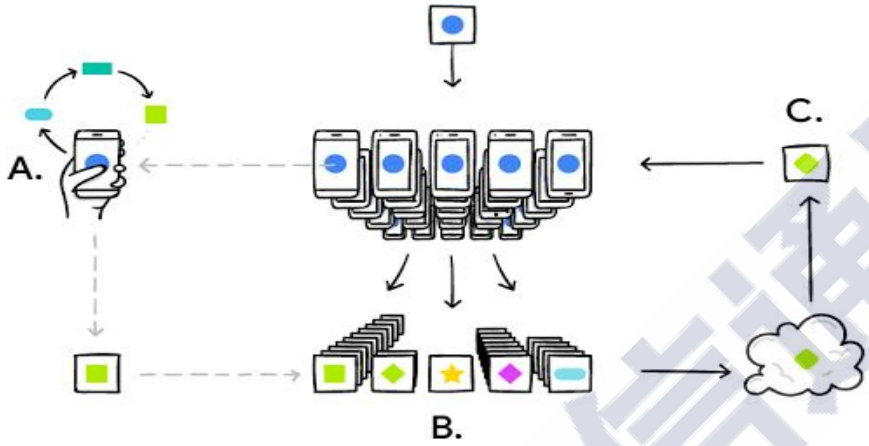
（一）联邦学习

1. 联邦学习定义

联邦学习（Federated Learning，FL）最初是由谷歌的 H.Brendan McMahan 等人提出[11]，并将其应用落地。即通过一个中央服务器协调众多结构松散的智能终端实现语言预测模型更新[12]（如图 3 所示）。其工作原理是：客户终端从中央服务器下载现有预测模型，通过使用本地数据对模型进行训练，并将模型的更新内容上传至云端。训练模

[11] Mcmahan H B , Moore E , Ramage D , et al. Communication-Efficient Learning of Deep Networks from Decentralized Data[J]. 2016.
[12] Federated Learning: Collaborative Machine learning without centralized training data, Google AI Blog. https://ai.googleblog.com/2017/04/federated-learning-collaborative.html

型通过将不同终端的模型更新进行融合，以此优化预测模型，客户终端再将更新后的模型下载到本地，过程不断重复。在整个过程中，终端数据始终存储在本地，不存在数据泄露的风险。



来源：Google AI

图 3　基于联邦学习的语言预测模型更新

联邦学习通常可以理解为是由两个或以上参与方共同参与，在保证数据方各自原始数据不出其定义的安全控制范围的前提下，协作构建并使用机器学习模型的技术架构。

联邦学习本质上来说是以数据收集最小化为原则，在保持训练数据去中心化分布的基础上，实现参与方数据隐私保护的特殊分布式机器学习架构，且基于联邦学习协同构建的机器学习模型与中心化训练获得的机器学习模型相比，性能几乎是无损的。但因其应用场景的不同，也使得联邦学习具有一些区别于传统分布式学习的特性：

● **数据的绝对掌控。**数据方作为模型训练的数据属主，对本地数据拥有绝对控制权，可自主决定何时加入、何时停止参与计算和通信。

● **参与方不稳定。**由于联邦学习不同参与方在计算能力、通信稳定性等方面存在差异，导致联邦学习相较于传统分布式机器学习存在参与方不稳定的情况。

● **通信代价高。**由于联邦学习参与方的不稳定，使得通信代价成为联邦学习的效率瓶颈之一。

● **数据非独立同分布。**在联邦学习中，不同参与方数据分布不同。如特征分布倾斜、标签分布倾斜、标签相同特征不同、特征相同标签不同等，不满足独立同分布。

● **负载不均衡。**各参与方数据在量级上存在差异化，各参与方的数据量不平衡，且在联邦学习中无法进行负载均衡。

2. 联邦学习分类

根据训练数据在不同数据方之间的特征空间和样本空间的分布情况，将联邦学习分为横向联邦学习（Horizontal Federated Learning，HFL）、纵向联邦学习(Vertical Federated Learning，VFL)和联邦迁移学习（Federated Transfer Learning, FTL）[13]。

横向联邦学习（Horizontal Federated Learning，HFL）：横向联邦学习主要是指在各参与方的数据集特征重合较大，但是样本重合较小的场景下，对应的联邦学习模式称之为横向联邦学习（图 4）。横向联邦学习的本质就是通过扩充样本数目，实现基于样本的分布式模型训练，以此达到模型效果提升的目的。

[13] 《联邦学习》，电子工业出版社。



来源：《联邦学习》，电子工业出版社

图 4　横向联邦学习

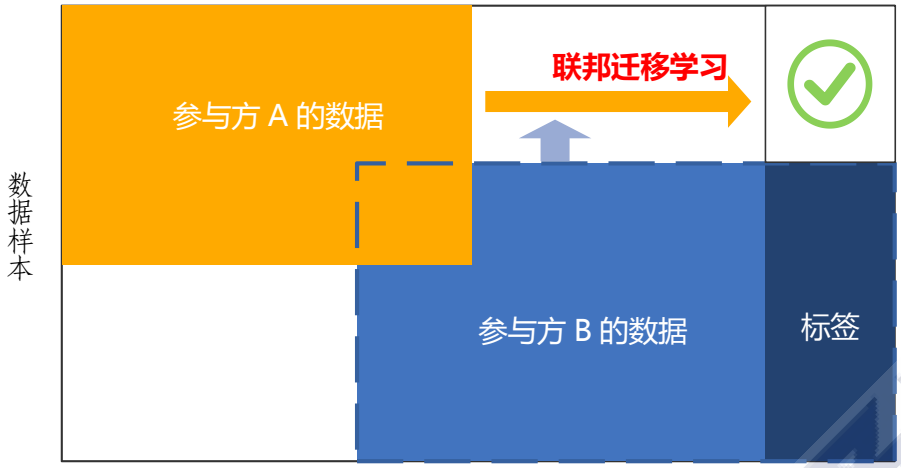
纵向联邦学习(Vertical Federated Learning，VFL)：与横向联邦学习不同，纵向联邦学习适用于在参与方数据集的样本重合度较高，但是特征重合度较低场景下，对应的联邦学习模式称为纵向联邦学习（图 5）。纵向联邦学习的本质是通过丰富样本特征维度，实现机器学习模型的优化。



来源：《联邦学习》，电子工业出版社

图 5　纵向联邦学习

联邦迁移学习（Federated Transfer Learning，FTL）：联邦迁移学习是指在各参与方的样本和特征重合度都极低的情况下，模型训练时，各数据集的样本空间与特征空间重叠范围都非常小时，相应的联邦学习称为联邦迁移学习（图 6）[13]。



来源：《联邦学习》，电子工业出版社

图 6　联邦迁移学习

3.　联邦学习参考架构

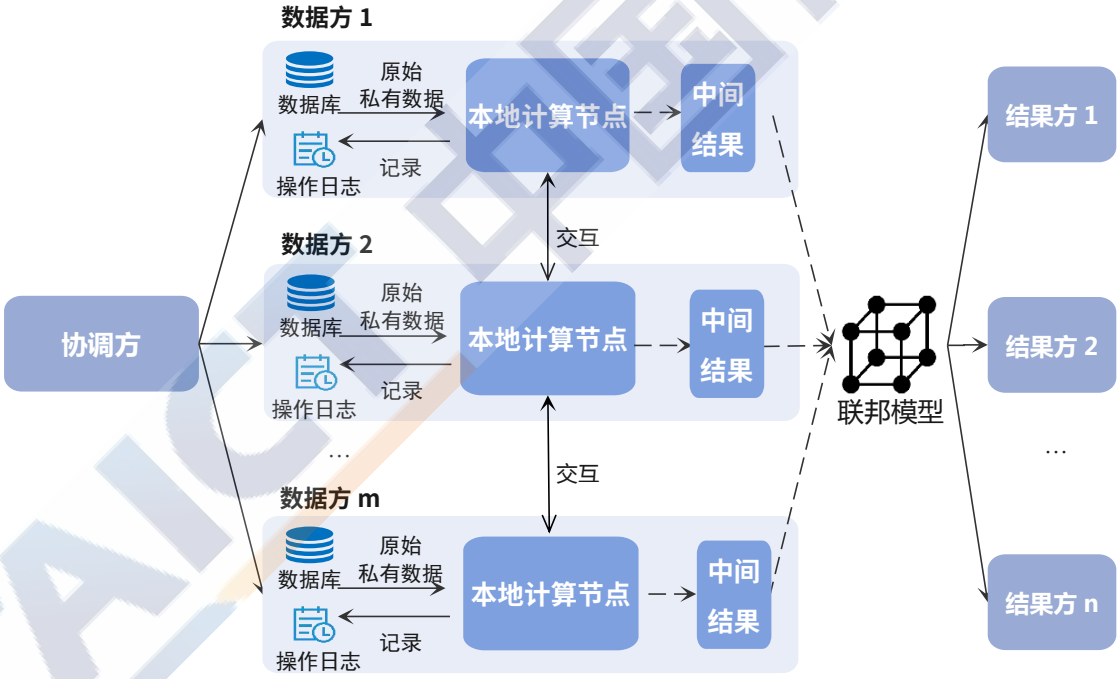


图 7　联邦学习参考架构

在联邦学习中，参与方主要承担的角色有协调方、数据方和结果方（如图 7 所示）。数据方是指提供联邦模型建模所需的私有数据的参与方；协调方是协调各参与方协作构建并使用联邦模型的参与方；结果方是指获取联邦学习结果的参与方。一个联邦学习参与方可承担

多个角色。例如一个参与方可以同时承担协调方、数据方和结果方三类角色。在联邦学习过程中，根据具体应用场景的不同，算力可以由数据方、协调方或者其他第三方提供。联邦学习支持的常见算法包括SecureBoost[14]、线性回归、逻辑回归、神经网络算法等。

4. 联邦学习安全属性

联邦学习的优势是以原始数据不出本地、共享数据最小化为根本遵循，实现一定程度的隐私保护。通常情况下，联邦学习主要提供安全性的隐私保护。

安全性（Security）[15]：理想情况下，联邦学习在模型训练和推理阶段，参与方只能获得其参与计算所必需的数据和协议规定的计算结果，不应获得其他任何信息。实际上为了兼顾实用性、公平性等，通常会在理想情况下做出一定的妥协。

安全性重点关注基于交互数据能否实现对参与方原始数据和隐私信息的推断。

5. 联邦学习开放问题

虽然现有的联邦学习解决方案已提供部分安全性的保护能力，但是在联邦学习中仍具有一些开放性的问题值得讨论。

在通信效率方面。传统分布式机器学习中，服务器之间的网络连接状态稳定可控，数据满足独立同分布，能有效实现负载均衡；而在

[14] Cheng K, Fan T, Jin Y, et al. SecureBoost: A Lossless Federated Learning Framework[J]. arXiv, 2019.
[15] Advances and Open Problems in Federated Learning[J]. 2019.

联邦学习中，各参与节点计算能力不一致、网络连接状态不稳定、数据通常非独立同分布，导致联邦学习的通信效率极易成为联邦学习应用的瓶颈之一。谷歌提出的 FedAvg[11] 算法是一个很好的起步点，但是有研究表明 FedAvg 的通信效率与模型收敛速度成反比[16]。其次，当前许多联邦学习方案引入部分同态加密等技术来加密保护中间值，加密会带来额外的计算代价，而且密文体积较大，这会进一步对效率造成不利影响。最后，FedAvg 等方案是针对横向联邦学习设计的，而面向纵向联邦学习的研究还相当欠缺。总而言之，如何设计方案以取得通信效率和收敛速度的平衡，这将是学术界和产业界关注的焦点。

在安全性方面。关于联邦学习的安全性并没有严格定义。通常希望达到实用性、安全性的平衡，已有部分针对联邦学习的安全性分析工作。**一是由梯度带来的隐私泄露。**由于梯度的本质是基于原始输入数据的函数 $\nabla W_{t,i} = \frac{\partial l(F(x_{t,i}, W_t), y_{t,i})}{\partial W_t}$，虽然原始数据没有出库，但是梯度几乎是包含原始数据信息的，所以一定程度上可以反推其他参与方的原始数据。无论是简单的逻辑回归[17]或是复杂的 CNN[18]，学术界已给出一些安全性分析论文，指出梯度泄露可能存在原始数据泄露的风险。部分解决方案采用了差分隐私技术实现梯度的隐私保护，但差分隐私保护技术是通过添加噪声实现隐私保护，不仅会使得机器学习模型收敛速度降低，而且会对模型的精度产生损失。在金融风控等对模型精度有较高要求的场景下是否可接受仍值得讨论。**二是隐私求交问题。**

---

16 Li X, Huang K, Yang W, et al. On the Convergence of FedAvg on Non-IID data[J]. arXiv preprint arXiv:1907.02189, 2019.

17 Li Z, Huang Z, Chen C, et al. Quantification of the Leakage in Federated Learning[J]. arXiv preprint arXiv:1910.05467, 2019.

18 .Zhu L, Liu Z, Han S. Deep leakage from gradients[C]//Advances in Neural Information Processing Systems. 2019: 14774-14784.

在纵向联邦学习中，基于隐私求交 PSI（Private Set Intersection，PSI）实现样本 ID 的对齐，能够对非交集内的样本 ID 进行保护，但交集内的明文样本 ID 存在泄露的风险。**三是基于半同态加密技术的单向隐私保护问题。**部分纵向联邦学习方案采用半同态加密技术对中间结果进行加密，但是这类方案中存在解密过程，因此仅能实现对私钥持有方单向的隐私保护。

在健壮性（Robust）方面。由于联邦学习本质上是一种分布式机器学习，所以也面临着拜占庭将军问题[19]。参与方中的敌手可在模型训练和模型推理阶段进行投毒攻击（Data Poisoning Attacks）以及逃逸攻击（Evasion Attacks）[15]等，以此来降低模型的性能或为模型预留后门等，破坏模型的可用性。目前关于健壮性讨论尚处在理论研究阶段，产业界考虑的较少。

（二）安全多方计算

1. 安全多方计算定义

安全多方计算（Secure Multi-Party Computation，SMPC）最早是由图灵奖获得者、中国科学院院士姚期智于 1982 年正式提出，解决一组互不信任的参与方各自持有秘密数据，协同计算一个既定函数的问题[20]。安全多方计算在保证参与方获得正确计算结果的同时，无法获得计算结果之外的任何信息。在整个计算过程中，参与方对其所拥

[19] Lamport L, Shostak R, Pease M. The Byzantine generals problem[M]// Concurrency: the Works of Leslie Lamport. 2019.
[20] YAO A C. Protocols for secure computation[C]. In Proc. of the 23rd Annual Symposium on Foundations of Computer Science, 1982.

有的数据始终拥有绝对的控制权。1986 年姚期智院士提出的针对两方计算的混淆电路方法成为构建通用 SMPC 协议的经典方案之一。后经 Goldreich, Micali 和 Widgerson 等学者进一步研究扩展到多方计算[21]，安全多方计算逐渐成为现代密码学的一个重要分支。

具体来说（图 8），在一个分布式网络中，有 n 个互不信任的参与方 P_1，P_2,…，P_n，每个参与方 P_i 持有秘密数据 $x_i(i=1,2,\ldots,n)$。这 n 个参与方协同执行既定函数 $f:(x_1,x_2,\ldots,x_n)\rightarrow(y_1,y_2,\ldots,y_n)$，其中 y_i 为参与方 P_i 得到的输出结果。任意参与方 P_i 除 y_i 之外无法获得关于其他参与方 $P_j(i\neq j)$ 的任何输入信息。如果 $y_1=y_2=\ldots=y_n$，可简单表示为 $f:(x_1,x_2,\ldots,x_n)\rightarrow y$。

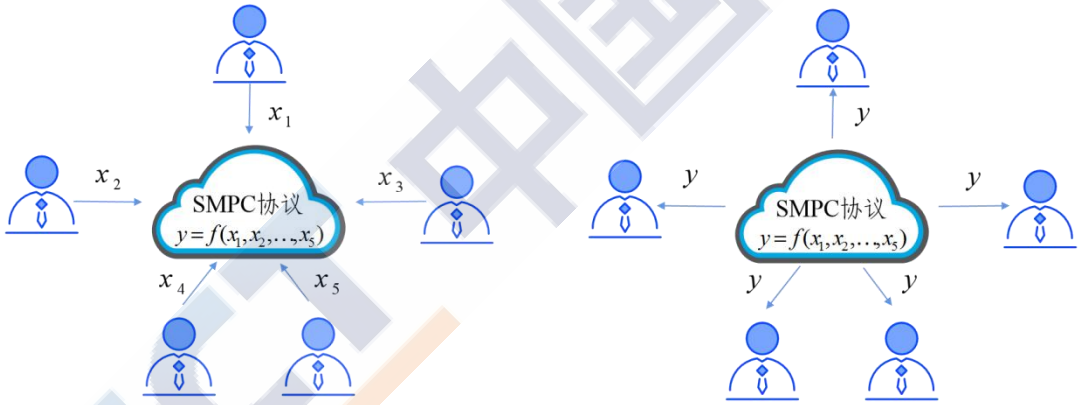


图 8　安全多方计算示意图

2.　安全多方计算安全属性

安全多方计算凭借其坚实的安全理论基础，实现了隐私保护计算过程安全性的严格定义。安全多方计算的属性主要包括输入隐私性、正确性、公平性和结果传递保证等。

输入隐私性（Input Privacy）：各参与方除自身输入的秘密数据

[21] Goldreich O, Micali S, Widgerson A. How to play any mental game[C]. In Proc. Of the nineteenth annual ACM symposium on Theory of computing, 1987.

以及既定函数计算输出结果外，无法获得其他任何信息。

正确性（Correctness）：若各参与方均遵守协议完成了计算，那么所有用户都应该收到各自计算函数的正确输出结果。

公平性（Fairness）（**可选**）：恶意参与方获得计算输出结果，当且仅当其他遵守 SMPC 协议的参与方都已获得计算输出结果。

结果传递保证（Guarantee Output Delivery）（**可选**）：遵守 SMPC 协议的参与方可以确保收到正确的计算结果。

3. 安全多方计算安全模型

当前，存在多种维度来评价安全多方计算方案安全性，其中最主要的是**行为模型**和**安全门限**。

3.1 行为模型

根据安全多方计算参与方的可信程度，可将安全多方计算的行为模型分为**半诚实敌手模型**和**恶意敌手模型**。

半诚实敌手模型（Semi-Honest Adversary Model）：各参与方严格遵循协议的要求，执行协议要求的各项步骤，但是会尽可能从获得数据中挖掘其他参与方的隐私。

恶意敌手模型（Malicious Adversary Model）：恶意参与方试图通过改变协议甚至采取任意的行为获取其他参与方的隐私。

满足恶意敌手模型的 SMPC 协议可以抵抗更强的攻击。

3.2 安全门限

假设一个 SMPC 协议的总参与方数目为n，根据安全多方计算参与方是否有合谋可能，可将安全多方计算的安全门限分为**诚实大多数**和**不诚实大多数**:

诚实大多数（Honest Majority）：可能合谋的人数小于$n/2$。

不诚实大多数（Dishonest Majority）：可能合谋的人数大于等于$n/2$。

满足不诚实大多数的 SMPC 协议可以抵抗更强的合谋可能。

就数据挖掘、机器学习这类典型隐私保护计算应用而言，目前市场上的大部分安全多方计算产品能够在半诚实敌手模型和诚实大多数假设下保持安全性，但满足恶意敌手模型或不诚实大多数假设则需要付出较大的性能代价，主要见诸于学术研究，而业界应用中尚不常见。

4. 安全多方计算关键技术

4.1 秘密共享（Secret Sharing，SS）

4.1.1 秘密共享定义

秘密共享作为现代密码学的重要分支，不仅是保护数据安全的重要手段，也是安全多方计算的基础应用技术之一。秘密共享通过将秘密信息分割成若干**秘密份额**并分发给多人掌管，以此来达到风险分散和容忍入侵的目的。一般来说，一个秘密共享方案由一个**秘密分割算**

法和一个**秘密重组算法**构成，包含**秘密分发者**、**秘密份额持有者**还有**接收者**三类角色[22]。**秘密分发者**持有秘密信息并且负责执行秘密分割算法，并将秘密份额分发给秘密份额持有者。接收者是试图重组秘密信息的一方。当接收者希望重组秘密信息时，将从一组授权的秘密份额持有者中收集秘密份额，并执行秘密重组算法计算秘密信息，当有充足的秘密份额就可以重新恢复出秘密信息。一个参与方可以同时承担多个角色。

4.1.2 秘密共享属性

消息机密性（Message Confidentiality）：秘密共享的消息机密性是指如果一组秘密份额持有者所拥有的秘密份额子集不足以进行秘密信息重组，那么该组秘密份额持有者就无法获得关于秘密消息的任何信息。

消息可恢复性（Message Recoverability）：秘密共享的消息可恢复性是指如果一组秘密份额持有者有足够进行秘密重组的秘密份额子集，则这些秘密份额持有者可以通过合并他们的秘密份额并应用消息重组算法对秘密信息进行重组。

4.2 不经意传输（Oblivious Transfer，OT）

不经意传输作为安全多方计算的重要基石之一，最初由 Rabin 于 1981 年提出[23]。如图 9 所示，该协议中发送方 Alice 拥有两个秘密消

[22] ISO/IEC 19592-1:2016 Information technology – Security techniques – Secret sharing – Part 1: General
[23] Rabin M O. How to exchange secrets with oblivious transfer[J]. Technical Report (Harvard University) ,2005.

息 x_0 和 x_1，接收者 Bob 选择并且仅能恢复其中的一个秘密消息 $x_b(b \in \{0,1\})$，但无法得到关于 x_{1-b} 的任何消息，Alice 无法知晓接收方选择的是哪一个消息。

现有的 OT 协议只能用公钥密码系统来实现，公钥密码系统相对对称密码系统来说一般性能低很多，无法适用于大规模数据传输的场景。例如很多安全多方计算方案中需要 Alice 和 Bob 频繁大量地传输 OT 消息，这时直接使用普通的 OT 协议的性能将难以接受。

为了解决这种大数据传输的场景，研究者提出了 OT Extension 协议：在 OT Extension 中，Alice 和 Bob 先执行少量的普通 OT 协议来传送较短的密钥种子。然后运行扩展（Extension）协议，通过对称密码算法把普通 OT 阶段的结果延长。这样整个过程主要使用的是高效的对称密码算法，仅第一阶段使用了少量的公钥密码计算，因此可以适配于大数据传输的场景。这种设计思想类似于信封加密系统中先用公钥传输对称密钥，再用对称密钥加密传输大文件。

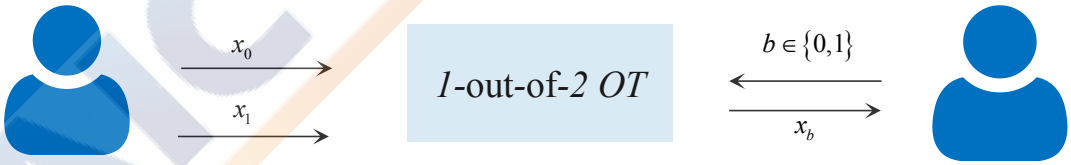


图 9　2 取 1 不经意传输协议

4.3 混淆电路（Garbled Circuit，GC）

混淆电路是由姚期智先生于 1986 年提出针对半诚实敌手模型的两方安全计算协议[24]，其核心思想是将任何函数的计算问题转化为由

[24] Yao C C . How to generate and exchange secrets[C]// Symposium on Foundations of Computer Science. IEEE, 2008.

“与”门、“或”门和“非”门组成的布尔逻辑电路，再利用加密技术构建加密版本的布尔逻辑电路。姚氏混淆电路包含布尔逻辑电路构建和布尔逻辑电路计算两部分。下面以“与”门（AND 门）为例简单说明姚氏混淆电路的主要思想，见图 10。复杂电路就是将一个个门电路串起来。假设 Alice 的秘密输入比特为 a，Bob 的秘密输入比特为 b，他们一起计算 AND 门，即 $a\&b$，分为电路构建和电路计算两部分。

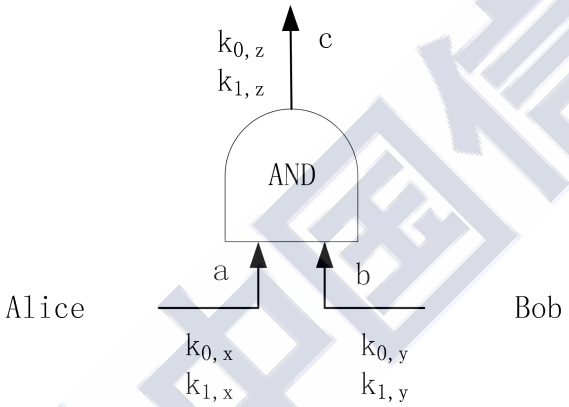


图 10　AND 门混淆电路示意图

电路构建： Alice 给每个电线随机选择两个密钥：$\{k_{0,x},k_{1,x}\}$，$\{k_{0,y},k_{1,y}\}$ 和 $\{k_{0,z},k_{1,z}\}$，其中 $k_{0,x}$ 对应 Alice 的输入 $a=0$，其他符号类似。Alice 构造加密真值表 $\begin{pmatrix}\mathrm{Enc}_{k_{0,x},k_{0,y}}(k_{0,z})\\ \mathrm{Enc}_{k_{0,x},k_{1,y}}(k_{0,z})\\ \mathrm{Enc}_{k_{1,x},k_{0,y}}(k_{0,z})\\ \mathrm{Enc}_{k_{1,x},k_{1,y}}(k_{1,z})\end{pmatrix}$，并随机打乱顺序得到混淆的加密真值表，如 $\begin{pmatrix}\mathrm{Enc}_{k_{1,x},k_{0,y}}(k_{0,z})\\ \mathrm{Enc}_{k_{1,x},k_{1,y}}(k_{1,z})\\ \mathrm{Enc}_{k_{0,x},k_{0,y}}(k_{0,z})\\ \mathrm{Enc}_{k_{0,x},k_{1,y}}(k_{0,z})\end{pmatrix}$。Alice 将混淆的加密真值表发送给 Bob。

电路计算： Alice 将$k_{a,x}$发送给 Bob，Bob 通过不经意传输协议获得$k_{b,y}$。Bob 使用$k_{a,x}$和$k_{b,y}$对混淆的加密真值表进行解密得到$k_{c,z}$。Bob 将$k_{c,z}$发送给 Alice。如果$k_{c,z}=k_{0,z}$，那么输出结果$a\&b=0$；如果$k_{c,z}=k_{1,z}$，那么输出结果$a\&b=1$。Alice 将结果分享给 Bob。

5. 安全多方计算解决方案部署实施

5.1 安全多方计算参考架构

在实际的安全多方计算工程部署中，参与方主要承担的角色包括数据方、计算方、结果方。数据方指原始秘密输入数据的提供者；计算方指安全多方计算协议算力的提供者，负责安全多方计算协议的实际执行；结果方指安全多方计算结果的接收方。

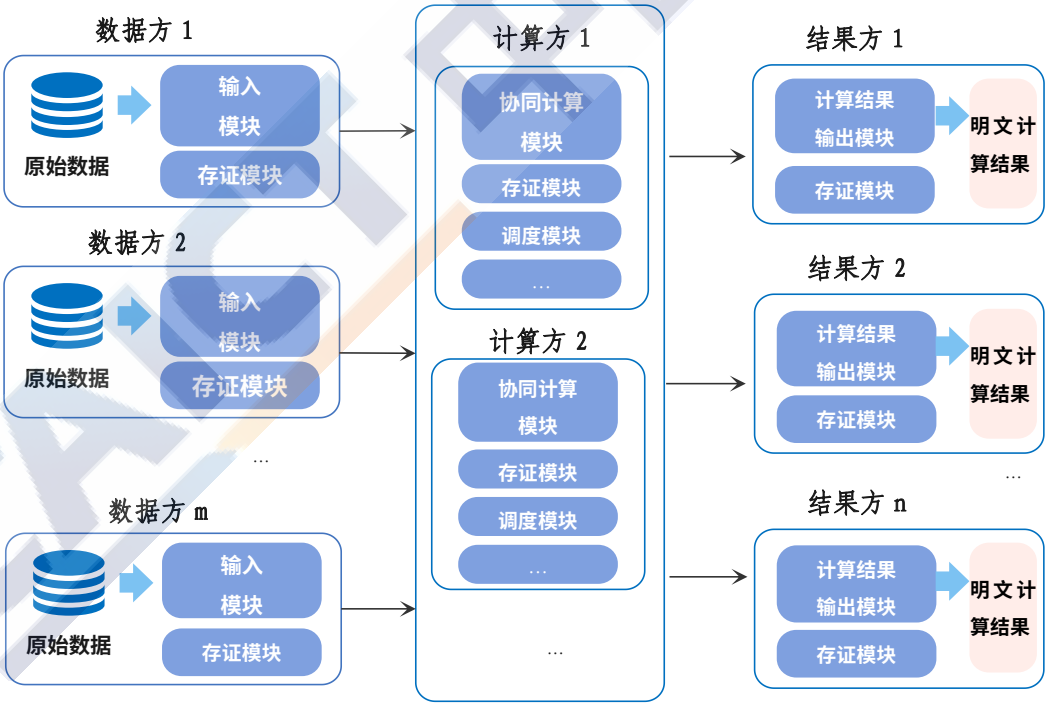


图 11　安全多方计算参考架构

在一次安全多方计算任务中，数据方按照预先设定的输入方式，

通过安全信道将数据发送给计算方；计算方接收数据方发送的数据，按照安全多方计算协议进行协同计算，并将结果发送给结果方。在安全多方计算协议中结果方可以有一个或多个，计算方为一个或多个。一个安全多方计算参与者可以同时担任多个角色。例如一个参与者可以同时承担数据方、计算方和结果方三类角色。

5.2 安全多方计算技术路线

安全多方计算凭借其坚实的安全理论基础提供输入秘密数据的隐私保护能力，实现隐私保护计算过程的安全。目前安全多方计算主要有两条实施技术路线，包括**通用安全多方计算**和**特定问题安全多方计算**。前者可以解决各类计算问题，但是这种“万能型”的技术路线通常体系庞大，各种开销较大；后者针对特定问题设计专用协议，如隐私集合求交 PSI（Private Set Intersection，PSI），隐私信息检索（Privacy Preserving Information Retrieval，PIR）等，往往能够以比通用安全多方计算协议更低的代价得到计算结果，但是需要领域专家针对应用场景进行精心设计，无法适用于通用场景且设计成本较高。

5.2.1 通用安全多方计算

通用安全多方计算解决方案主要包括**基于秘密共享的安全多方计算解决方案**、**基于混淆电路的安全多方计算解决方案**以及**基于全同态加密的安全多方计算解决方案**。但基于全同态加密的安全多方计算目前仍处在理论研究阶段，距离实际应用仍存在一定的差距。综合考

虑实际场景的应用效果，目前在各领域中应用较为广泛的是基于秘密共享和基于混淆电路的安全多方计算方案。

● **基于秘密共享的安全多方计算解决方案：**基于秘密共享的安全多方计算解决方案采用基于秘密共享的方式实现各类通用计算，中间计算值以秘密份额的方式存在。在此基础上进行应用层算法的指令改写，构造安全多方计算的电路实现秘密份额上的基本运算，如加法、乘法、比较等。基于秘密共享方法的 SMPC 协议通信轮数与电路的深度成线性关系，所以在相同的计算需求背景下，通信轮数更多。

● **基于混淆电路的安全多方计算解决方案：**基于混淆电路的安全多方计算解决方案其通信轮数与电路深度无关，因此在机器学习训练等较深的电路需求背景下，总通信轮数更少，但总通信量更大。

一般来说，基于混淆电路方法的 SMPC 更适合高带宽的网络，而基于秘密共享的 SMPC 协议适合低延迟的网络。此外，基于秘密共享的方案可以高效的支持加法和乘法等算术运算，但难以高效支持复杂的运算如浮点计算；而基于混淆电路的方案理论上可以通过门电路实现任意逻辑运算，但由于其通信量较大，对网络带宽要求较高。因此在流行的安全多方计算解决方案,如 SecureML[25]中，经常采用基于秘密共享的方案实现加法和乘法，而对于更加复杂的执行逻辑（如 RELU、SIGMOID 等），则采用基于混淆电路的方案。

[25] Mohassel P, Zhang Y. SecureML: A system for scalable privacy-preserving machine learning[C]. 2017 IEEE Symposium onSecurity and Privacy (SP), 2017

表 1　通用安全多方计算实施方案对比

	基于秘密共享的安全多方计算解决方案	基于混淆电路的安全度多方计算解决方案
通信量	少	多
通信轮数	多	少
简单算子性能（如加法、乘法等）	高	低
复杂算子性能（如指数、对数等）	低	中

5.2.2 特定问题安全多方计算

在学术界和具体应用场景中，已经有不少针对特定问题的安全多方计算解决方案，比如隐私集合求交集（Private Set Intersection，PSI）、隐私信息检索（Privacy Preserving Information Retrieval，PIR）、安全多方统计（Privacy Preserving Statistical Analysis，PPSA）、保护隐私的数据挖掘（Privacy Preserving Data Mining，PPDM）等。下面主要介绍 PSI 和 PIR。

● **隐私集合求交集 PSI**：PSI 指通过一系列底层的密码学技术，允许参与方使用各自的数据集合计算交集，且不会泄露交集以外的任何数据，在黑名单共享、营销匹配等现实场景中有广泛应用。近些年 PSI 技术在理论和工程实现上均得到迅猛发展，一些 PSI 协议可以达到上亿量级的数据处理能力。根据底层所用技术的不同，PSI 可以分为**基于公钥加密机制的 PSI**、**基于电路的 PSI** 和**基于不经意传输协议的 PSI 三类**。一般地，基于公钥加密机制的 PSI 通信复杂度和计算复杂度都与集合大小成线性关系，虽然通信复杂度在几类 PSI 中最低，但是计算开销随着集合增大变得非常高；由于计算交集的整个逻辑

（或算术）电路的门数和深度很大，基于电路的 PSI 计算效率很低；随着 OT 协议的快速发展，基于 OT 协议的 PSI 在时间复杂度和通信复杂度均得到很大提升，特别适用于大规模数据交集计算。目前，基于公钥加密机制的 PSI 由于其原理的简洁性，在工业中的应用较为广泛。

如上文“联邦学习的开放性问题”所述，PSI 可以保护非交集数据，但是不可避免的泄露了交集部分数据。针对此问题，Facebook 发布了一种新的 PSI 方案 PS^3I[26]，可以计算得到交集的秘密共享结果，进一步保护了交集部分的隐私内容。

● **隐私信息检索 PIR**：PIR 是客户端从数据库检索信息的一种方法，且数据库无法知道客户端检索的具体信息，保护客户端的隐私安全。一个简单的实现方案是数据库把所有数据发送给客户端，但是通信复杂度是线性的，且无法保护数据库安全。因此 PIR 的一个重要目标是降低协议执行过程中的通信复杂度。此外，能够同时保证客户端和数据库隐私安全的 PIR，称为对称的 PIR（Symmetrical PIR，SPIR）。根据数据库副本的个数分为多副本 PIR 和单副本 PIR。多副本 PIR 协议要求多个数据库副本之间不能合谋，这在现实场景中很难满足，因此考虑更多的是单副本 PIR。单副本 PIR 只能达到计算安全（Computational PIR，CPIR）。在大多数 PIR 方案中，总是假设客户端知道想要检索的是数据库的第几个比特（单比特）。但是在现实场景中，客户端往往是根据关键字检索（并不知道该关键字对应数据库

[26] Private matching for compute: New solutions to the problem of enabling compute on private set intersections https://engineering.fb.com/open-source/private-matching/

的具体位置），且希望取回的是字符串（多比特）。总而言之，一个实用的 PIR 通常需要满足对称、单副本、按关键字检索、返回字符串等多个条件，并达到计算效率和通信效率的平衡。通过同态加密、OT、单向陷门函数等密码学技术，可以满足或部分满足上述条件。

（三）机密计算

机密计算（Confidential Computing）是一种基于硬件可信执行环境实现数据应用保护的技术[27]。2019 年 8 月，Linux 基金会宣布成立由埃森哲（Accenture）、蚂蚁集团、ARM、谷歌、Facebook、华为、微软、红帽等多家巨头企业组建的“机密计算联盟”（Confidential Computing Consortium，CCC）[28]。该联盟针对云服务及硬件生态，致力于保护数据应用中的安全。

1. 机密计算定义

在机密计算联盟定义前，已有相关机构对“机密计算”进行了定义。如 Gartner 在 2019 年隐私成熟度曲线报告[29]中将机密计算定义为“机密计算是一种将基于 CPU 硬件技术、IaaS 云服务提供商虚拟机镜像以及相关软件进行组合，使得云服务消费者能够成功创建隔离的可信执行环境，也称作 Enclave。由于提供了数据使用中的加密形式，这些 Enclave 使得敏感信息对主机 OS 和云提供商不可见。”可信计算联盟认为除了云计算场景外，机密计算应该包含更广泛的应用场景。

[27] Confidential Computing Deep Dive v1.0
[28] Confidential computing consortium https://confidentialcomputing.io/
[29] Gartne: Hype Cycle for Privacy, 2019

此外，采用“加密”的表述是不严谨的，因为“加密”技术仅作为实现数据隐私保护的技术之一，而不是唯一技术，机密计算所采用的技术应包含正在探寻中的其他技术。

据此，机密计算联盟将机密计算定义为“机密计算是指通过在基于硬件的可信执行环境中执行计算来保护数据应用中的隐私安全的技术之一”[27]。为了减少机密计算环境对特有软件的信任依赖，机密计算重点关注基于硬件可执行环境的安全保证。基于硬件的可信执行环境（Trusted Execution Environment，TEE）作为机密计算的核心技术，因其提供了一个基于硬件防护能力的隔离执行环境，近年来逐渐成为大家关注的焦点。遵循行业惯例，机密计算联盟将可信执行环境（TEE）定义为在数据机密性、数据完整性和代码完整性三方面提供一定保护水平的环境[27]。目前引入可信执行环境较为成熟的技术有ARM 的 TrustZone 和 Intel 的 SGX（Software Guard Extensions，SGX）等。

2. 机密计算成熟技术

2.1 TrustZone

TrustZone 将系统的硬件和软件资源划分为两个执行环境—安全环境（Secure World）和普通环境（Normal World），安全环境拥有更高的执行权限，普通环境无法对其进行访问，实现隔离的执行环境。当不安全的用户模式需要获取安全域的服务时，一个程序想要进入安全环境中，操作系统需要检查其安全性，只有通过检验的程序才能进

入安全环境，以此来确保 TrustZone 的安全性，这也意味着整个系统的安全性由底层操作系统来负责。

2.2 Intel SGX

SGX 是由 Intel 提出，基于 CPU 的实现执行环境隔离的新一代硬件安全机制。SGX 通过内置在 CPU 的内存加密引擎 MME（Memory Encryption Engine，MME）以及 Enclave 实现了应用程序运行安全和数据安全。Intel SGX 允许应用程序实现一个被称为 Enclave 的容器，在应用程序的地址空间划分出一块被保护的区域，将合法软件的安全操作封装在 Enclave 中，为容器内的代码和数据提供机密性和完整性保护，免受拥有特权的恶意软件的破坏。当应用程序需要保护的部分加载到 Enclave 后，保证只有位于 Enclave 容器内部的代码才能访问 Enclave 所在的内存区域，容器之外的任何特权和非特权软件都不能访问 Enclave 内部数据。所有的 Enclave 都驻留在 EPC（Enclave Page Cache，EPC）中，EPC 是系统内分配的一块被保护的物理区域。

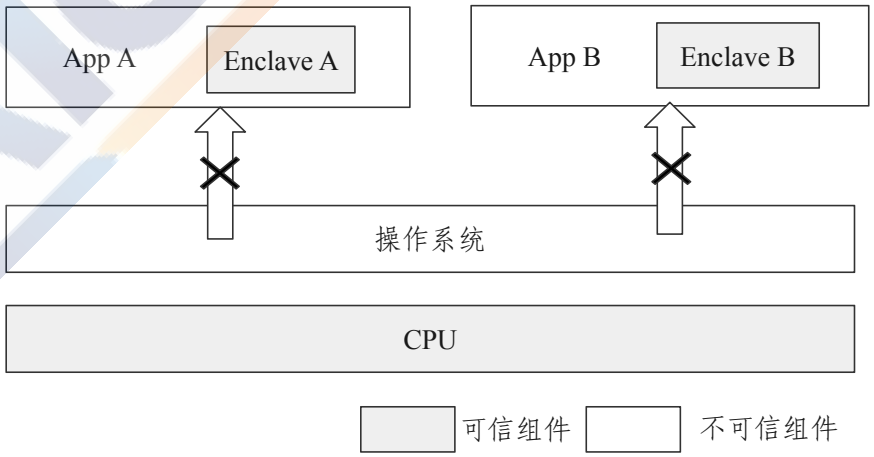


图 12　Intel SGX 基本原理

不同于 ARM 的 TrustZone，Intel 的 SGX 可信计算基缩小至 CPU，支持一个 CPU 上运行多个 Enclave，相较将操作系统或特权软件作为可信计算基的 TrustZone，Enclave 彼此相互独立，减少了潜在的攻击面，防止由单个恶意程序影响整个系统安全性。

3. 机密计算开源框架

由于目前服务器领域依然被 x86 架构主导，而 ARM 架构目前主要应用在手机、平板等低功耗设备，难于适用于大规模数据共享。因此，主流的机密计算开源框架大多是基于 Intel SGX 的。具体包括 Rust SGX SDK、Asylo（不限于 SGX）以及基于 libOS 的机密计算开源框架。

3.1 Rust SGX SDK

尽管 Intel SGX 能够保护重要应用程序的安全性，但是这些应用程序使用如 C/C++等不安全的语言开发，仍然可能存在传统的内存安全漏洞。Rust SGX SDK 是一个由百度安全实验室发起的开源项目，它将 Rust 语言和 Intel SGX 技术进行结合，可通过该项目用 Rust 语言编写 Intel SGX 应用程序[30]。得益于 Rust 语言的内存权限管理等优势，程序员可以基于该 SDK 开发出没有内存安全漏洞的 Intel SGX 可信程序，且性能几乎没有额外开销。

Rust SGX 分为三层（见图 13）[31]：（1）底层是 Intel SGX SDK，

[30] Rust SGX SDK：https://github.com/baidu/rust-sgx-sdk
[31] Wang H B, Wang P, Ding Y, et al. Towards memory safe enclave programming with Rust-SGX. CCS'19

用 C/C++实现，也可以用汇编实现；（2）中间层是 Rust 和 C/C++的 FFI（Foreign Function Interfaces）；（3）上层是 Rust SGX SDK。

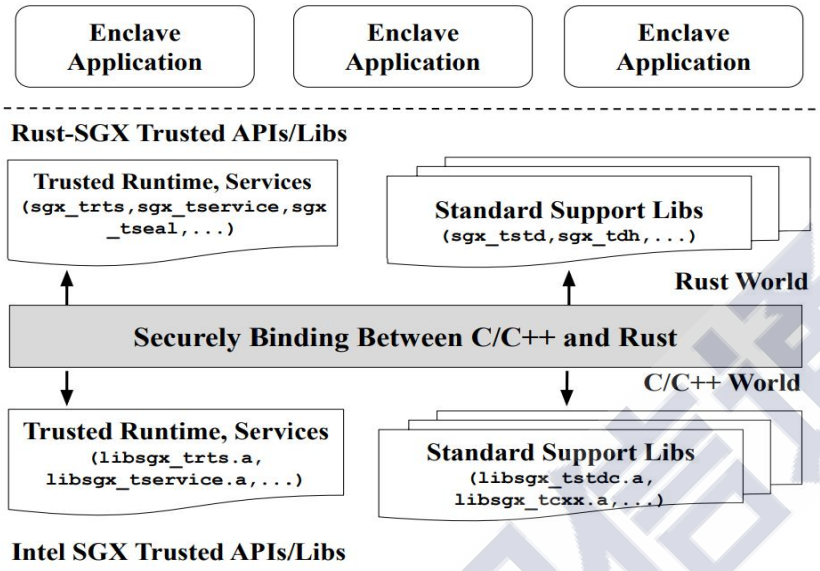


图 13　Rust SGX 架构示意图 [30]

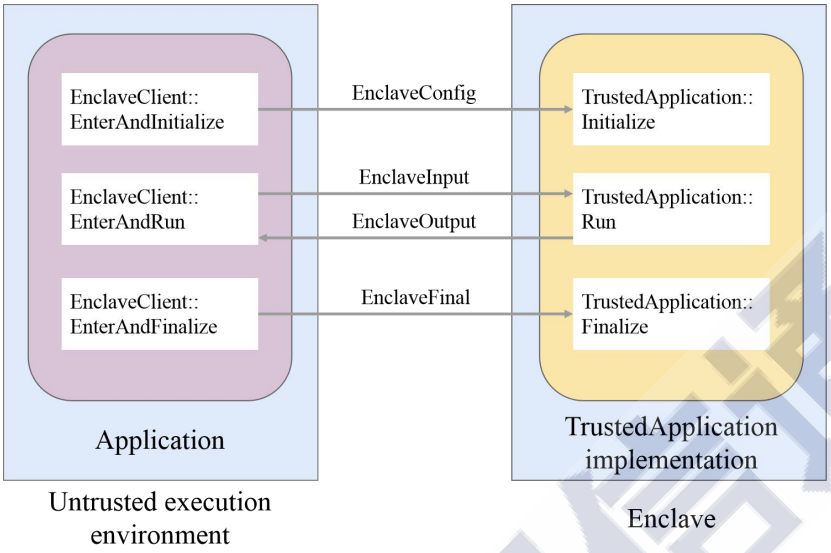
3.2 Asylo

Asylo[32]是谷歌发起的开源机密计算开发框架，它包含用于加密敏感通信的功能和服务。一般而言，在 TEE 中开发和运行软件需要专业的知识和工具，而且部署也需要与特定的硬件环境绑定。Asylo 框架的目标是使得更多的开发人员能够便捷的开发使用 TEE，并支持各种硬件——从企业内部系统到云端。

在 Asylo C++ API 中，Enclave 应用包含可信和不可信组件。开发和使用 Enclave 的类主要有：TrustedApplication、EnclaveClient 和 EnclaveManager。其中 TrustedApplication 是 Enclave 应用的可信组件，负责敏感的计算；EnclaveClient 是 Enclave 应用的不可信组件，负责

[32] Asylo: https://asylo.dev/

和可信组件的通信；EnclaveManager 是不可信系统中的单例对象，负责 Enclave 的生命周期管理和 Enclave 之间的资源共享。



来源：Asylo 官网

图 14　消息传递接口示意图

图 14 是消息传递接口示意图。可信环境包含一个或多个 Enclave，用来保护敏感工作负载中的代码和数据。创建一个 Enclave，需要定义从 TrustedApplication 继承的类，并将实现逻辑托管在 Enclave 中。类似地，不可信 API 提供必要的方法以便可以安全地进出 Enclave。进入 Enclave 类似于进行系统调用。Enclave 入口点实现了进入敏感代码的通道，以访问 Enclave 资源。进入时将参数复制到 Enclave，退出时将结果复制出来。

3.3 基于 libOS 的方案

除了使用 SDK 开发 TEE 程序之外，另外基于 libOS 的机密计算也开始流行。简单来讲，libOS 在真实的操作系统上层准备了一份精简的操作系统作为软件的运行库，为软件提供了隔离、方便迁移等优

势。为此，将 libOS 和主机的 OS 相互分离，使得两者能够快速和独立的进行升级，能够跨计算机迁移各个应用程序的运行状态，从而更好地保护系统和应用程序的完整性，每个应用程序之间都是相互独立的，只能通过 libOS 层面来进行通信。对于机密计算来说，libOS 的优点是可以便捷的将已有的程序迁移到 TEE 环境，而无需重新开发，其缺点是增大了可信计算基的内容（整个 libOS 可信）。目前支持 SGX 特性的 libOS 有 Graphene[33]、Occlum[34]等。这些 libOS 提供通用的系统调用接口，可以透明地处理需要调用系统软件的所有 Enclave 到不可信环境的转换。

机密计算通过基于硬件的可信执行环境实现了执行环境的隔离。本质上来说，机密计算的安全性与硬件本身的安全性是强相关的。尤其在当前国际经贸摩擦不断加剧，国际形势瞬息万变的格局下，对于通过采购国外的硬件产品实现隐私保护仍待商榷。疫情的冲击暴露出我国在供应链存在的风险隐患。为保障国家安全，我们要着力打造自主可控、安全可靠的供应链，争取做到诸如 TEE 芯片等安全相关产品实现自主替代。

（四）差分隐私

差分隐私（Differential Privacy，DP）被麻省理工科技评论为 2020 全球十大突破性技术之一[35]，在美国 2020 年人口普查中的应用成为迄

[33] Graphene: https://grapheneproject.io/

[34] Occlum: https://occlum.io/

[35] 《麻省理工科技评论》2020 年“全球十大突破性技术”

今为止差分隐私保护技术的最大规模应用，实现了在不损害个人隐私的前提下最大限度利用数据资源的核心诉求。

1. 差分隐私定义

差分隐私作为量化和限制个人信息泄露的一种输出隐私保护模型，最早是 Dwork[36]在 2006 年提出。在差分隐私中最关键的概念是相邻（adjacent）。假设有有两个数据集 D_1 和 D_2，他们有且仅有一条数据不一样，则称这两个数据集是相邻的。若一个算法 $\mathcal{A}$，$Range(\mathcal{A})$ 为算法 $\mathcal{A}$ 可能输出的所有值的集合，如果对于任意的一对相邻集合 D 和 D'，任何 $\mathcal{S} \subseteq Range(\mathcal{A})$ 都满足：

$$P(\mathcal{A}(D) \in \mathcal{S}) \leq e^{\varepsilon} P(\mathcal{A}(D') \in \mathcal{S})$$

则称算法 $\mathcal{A}$ 满足 ε-差分隐私保护[37]，记作 ε-DP。ε 为一个极小正值，代表隐私保护程度。一般而言 ε 越小，隐私保护程度就越高。

差分隐私最主要的实现方式是在计算结果中添加噪声。如适用于数值型输出的 Laplace 噪声等及适用于非数值型输出的指数噪声等。差分隐私具有两个最重要的优点。**一是**差分隐私严格定义了一个背景知识无关的隐私保护模型，实现了攻击者背景知识最大化假设，理论上能够抵抗任何攻击。**二是**差分隐私建立在严格的数学理论基础之上，对隐私保护进行了严格的定义并提供了量化评估方法，对隐私保护水平进行了科学严谨的证明。

---

[36] Dwork C . Calibrating noise to sensitivity in private data analysis[J]. Lecture Notes in Computer ence, 2012, 3876(8):265-284.

[37] Dwork C , Kenthapadi K , Mcsherry F , et al. Our Data, Ourselves: Privacy Via Distributed Noise Generation[C] // International Conference on Advances in Cryptology-eurocrypt. DBLP, 2006.

2. 差分隐私组合定理

差分隐私技术通常解决单个查询的隐私保护问题。但在实际中，经常需要面临多条隐私计算组合或在同一数据集重复执行相同的隐私计算的情况，能实现何种程度的隐私保护能力。差分隐私组合定理（Composition Theorem）的提出，目的就是将一系列满足差分隐私的计算组合，仍然保证整体满足差分隐私要求。

常见的组合定理包括串行组合与并行组合。串行组合（Sequential Composition）针对的是同一数据集不同计算函数，定义为[38]:

给定数据集 X，以及一组关于 X 满足 ε_i 的差分隐私的 k 个算法 $M_1(X), M_2(X), M_3(X), \cdots, M_k(X)$，任意两个算法 M_i 与 $M_j (1 \le j \ne i \le k)$ 的随机过程彼此独立，则这些算法的组合满足 $\sum_i^k \varepsilon_i$ -差分隐私。即针对同一数据集，执行多个不同的差分隐私算法组合的隐私保护程度的损失是可累加的。

并行组合（Parallel Composition）则针对的是不相交数据集上的不同计算函数。定义为:

数据集 X 的元素 x 定义在域 D 上，令 $\{D_1, D_i, \cdots, D_t\}$ 是 D 的一个划分，满足 $D = \cup_{i=1}^{t} D_i$ 且 $D_j \cap D_i = \varnothing$（$i \ne j$），$M_i (1 \le i \le k)$ 表示一个满足 ε 的差分隐私算法，$M_i(X \cap D_i)$ 表示各个差分隐私算法之间作用的数据集互不相交且彼此独立，那么关于算法 $M_i(X \cap D_i)$ 的组合也满足 ε 差分隐私安全。

相对于串行组合的隐私代价累计，并行组合的隐私保护程度的损失是相对固定的，独立于计算数量。

---

[38] McSherry, Frank. Privacy integrated queries[J]. Communications of the Acm, 2010, 53(9):89. .

3. 差分隐私分类

传统的差分隐私方案大多为中心化的差分隐私方案，即数据通常都是由可信第三方添加噪声。但在实际应用中为了减少对可信第三方的需求，近年来也提出了一些去中心化的隐私保护方案，如**本地差分隐私**等。

本地差分隐私（Local Differential Privacy，LDP）是在基于不可信第三方的前提下，客户端在数据被收集和聚合前，在本地对数据进行差分隐私保护。本地差分隐私已经被谷歌、苹果和微软等公司广泛应用。但是相较于传统中心化差分隐私，本地差分隐私方案对数据添加的噪声更大，在面向数据统计时数据的可用性更低。

差分隐私是一种建立在严格数学理论基础之上的隐私定义，旨在保证攻击者无法根据输出差异推测个体的敏感信息。即差分隐私必须提供输出结果的统计学不可区分性。但是在任何差分隐私算法中，随机性都是不可或缺的，所以任何确定性算法都无法满足差分隐私保护的不可区分性。差分隐私仅通过噪声添加实现隐私保护，虽然不存在额外的计算开销，但是对模型数据的可用性仍然会造成一定程度的影响。如何设计出能够更好地平衡隐私和可用性的方案也是未来关注的重点。

（五）同态加密

同态加密是一种特殊的加密算法，它允许在加密之后的密文上直接进行计算，且计算结果解密后正好与明文的计算结果是一致的。为

便于大家理解，举个同态加密非正式例子，如:

Encrypt(2)⊕Encrypt(3)=Encrypt(2⊕3)

Encrypt(2)⊙Encrypt(3)=Encrypt(2⊙3)

目前的同态加密实现多为非对称加密算法，即所有知道公钥的参与方都可以加密、执行密文计算，但只有私钥所有者可以解密。按照支持的功能划分，目前的同态加密方案可以分为**部分同态加密方案**（Somewhat Homomorphic Encryption，SHE）和**全同态加密方案**（Fully Homomorphic Encryption，FHE)两类:

部分同态加密方案（Somewhat Homomorphic Encryption，SHE）: 只能支持有限的密文计算深度，例如Paillier[39]支持密文间的加法运算，但是不支持密文间的乘法运算；BGN[40]能够支持无限次密文间的加法运算，但是只能支持一次密文间的乘法运算（乘法结果无法再支持密文乘法了）；由于 SHE 功能的局限性，一般很难完全基于 SHE 独立建设一个隐私保护计算方案，但是很多方案中会使用 SHE 来实现其某个子功能。例如联邦学习中，一种常用的方案就是基于 SHE 来做 Secure Aggregation。

全同态加密方案（Fully Homomorphic Encryption，FHE): 对密文上的计算深度没有限制，理论上可以支持任意的密文计算。自 2009 年 Gentry 首次提出基于理想格的 FHE 构造[41]以来，FHE 已经得到了突飞猛进的发展，尤其是支持近似小数计算的 CKKS 方案[42]的提出，

[39] Paillier P . Public-Key Cryptosystems Based on Composite Degree Residuosity Classes[J]. 1999.
[40] Boneh D . Evaluating 2-DNF Formulas on Ciphertexts[J]. TCC'05, 2005.
[41] Gentry, Craig. Fully homomorphic encryption using ideal lattices[J]. Stoc, 2009:169-178.
[42] Cheon J H , Kim A , Kim M , et al. Homomorphic Encryption for Arithmetic of Approximate Numbers[J]. 2017.

大大提升了在加密的数据上进行机器学习等计算的性能。理论上，我们可以完全基于 FHE 建设一个隐私保护计算方案，学术界也已经有了许多相关研究，但是 FHE 的计算代价仍然比较高，目前还未了解到有商业应用中实际应用了 FHE。

三、隐私保护计算关键技术综合评价

隐私保护计算作为涉及多领域交叉融合的跨学科技术体系，重点提供了数据计算过程和数据计算结果的隐私安全保护能力。但不同细分技术在理论基础、技术实施路线等方面有着较大的差异，故本章围绕保护效果、计算性能、计算精度、硬件依赖、理论支持场景、实际应用场景、计算模式七个维度对上述的技术进行对比总结（如表 2 所示）。

安全多方计算：由于 SMPC 其可证明的安全性，除了最终的计算结果之外严格没有任何信息泄露，因此受到密码学家的青睐。SMPC 包含复杂的密码学操作，因此实现 SMPC 需要付出很大的性能代价，但对于一些复杂度较低的场景（如密钥管理、简单统计、线性模型等），SMPC 已经能够在不少场景中取得可接受的应用效果。在计算场景较复杂（例如神经网络、GBDT 等）时，SMPC 的性能则仍然较差。SMPC 的性能瓶颈主要是通信耗时，其性能进步不仅依赖于底层理论突破，还受到网络带宽、延迟等因素制约。

联邦学习：联邦学习最初是由机器学习领域提出，其核心思想是各个参与方尽量在本地完成建模所需计算，仅在模型需要迭代更新时

进行通信交互。目前学术界对于联邦学习的安全保障效果尚无严格的定义。事实上现有的各类联邦学习方案也都难以保证模型更新过程中的零信息泄露。因此使用联邦学习方案进行机器学习建模，实质上是泄露了比最终模型更多的信息。虽然联邦学习的通信代价比 SMPC 低，但是其性能也很大程度上受到网络带宽、延迟等因素制约。

机密计算：与上述两类去中心化的方案相比，使用机密计算进行数据协同计算一般是将多方数据集中进行中心化的处理，除了硬件不同之外，与普通的数据计算并无本质不同，因此其不存在算法和网络瓶颈，性能更强。基于硬件的可信执行环境方案作为机密计算的核心技术，它的安全风险**首先**是来自对基于硬件的可信执行环境的各类侧信道攻击: 基于硬件的可信执行环境空间和操作系统其它非可信执行环境空间共享了大量的系统资源，因此攻击者可以通过这些共享资源进行侧信道攻击，并推导基于硬件的可信执行环境内部的机密数据内容。**其次**，使用基于硬件的可信执行环境方案必须要相信可信执行环境厂商是可信的。例如可信执行环境方案中的远程通信需要可信执行环境厂商参与远程证明。**最后**，如果要部署基于硬件的可信执行环境方案，需要购买指定的硬件，这在一些场景会显著的提高使用成本。

差分隐私：差分隐私的保护目标是计算结果而不是计算过程，因此它与上述三种方案有根本不同。以机器学习建模为例，差分隐私可以在建模结果上加入一定的噪声，保证攻击者难以从建模结果反推出训练样本的信息; 但是差分隐私依然需要计算方显式的访问训练数据，因此没有保护建模过程。也可以将联邦学习、安全多方计算、机密计

算方案和差分隐私进行结合，以达到同时保护计算过程和计算结果的效果。差分隐私的主要问题在于会对计算结果的准确度形成不可忽略的影响，针对某些对准确度不敏感的场景可行。但是对于诸如风险识别、人脸识别这类准确度要求较高的场景是难以接受的。

本地差分隐私：本地差分隐私则将计算方也视为不可信任的，数据在进入计算过程之前即已加入噪声，因此本地差分隐私能够同时保护计算过程和计算结果。本地差分隐私引入的误差比差分隐私更大，而且更大的问题是本地差分隐私处理过的数据目前只能支持有限的统计计算，难以用于机器学习建模等复杂场景。

同态加密：由于部分同态加密仅能支持有限的密文计算深度，因此常将部分同态加密方案作为其他方案的组成部分之一进行应用。而全同态加密方案由于性能瓶颈，目前的研究大多聚焦于学术层面，尚无商用案例。

表 2　关键技术综合评价表

	保护效果		计算性能	计算精度	硬件依赖	理论支持场景	实际已商用场景	计算模式
	计算过程保护	计算结果保护						
安全多方计算 SMPC	★★★★★	无	★★☆☆☆	★★★★★	无	任意计算	国外：拍卖、薪资统计、密钥管理； 国内：密钥管理、联合建模	分布式
联邦学习 FL	★★★☆☆	无	★★★☆☆	★★★★★	无	机器学习建模	国外：以横向 FL 为主，如谷歌 Gboard 国内：以纵向 FL 为主，在金融风控领域应用居多	分布式
机密计算 CC	★★★☆☆	无	★★★★★	★★★★★	有	任意计算	国外：密钥管理； 国内：联合建模、区块链；	中心化
差分隐私 DP	无	有	★★★★☆	★★★☆☆	无	任意计算	谷歌 Gboard	中心化
本地差分隐私 LDP	★★★★☆	有	★★★★☆	★★☆☆☆	无	数据统计	谷歌 Chrome/苹果 iPhone	分布式+中心化
全同态加密 FHE	★★★★★	无	★☆☆☆☆	★★★★☆	无	任意计算	未了解	中心化

CAICT 中国信通院

四、隐私保护计算应用案例

隐私保护计算能够为参与实体提供高效、安全的合作模式，各方在确保数据合规使用的情况下，实现数据共享和数据价值挖掘。因此在金融、政务、医疗等领域有着广泛的应用前景。

（一）金融领域

尽管金融数据在体量、维度、价值等方面具有一定优势，但是这部分数据更多涉及客户金融相关的数据，缺少客户的行为数据、场景数据等。具体到某一个金融机构时，其数据的丰富程度更大打折扣。而客户的行为数据和场景数据往往掌握在一些互联网公司和其他数据源公司手中。在**信贷风险评估、供应链金融、保险业、精准营销、多头借贷**等方面，金融机构都需要和这些数据源公司联合建模，提升模型的精确度。

但是金融数据的安全及风险防范一直是金融机构关注的重点，国家也相继出台金融安全相关政策，不断强化对金融数据安全的重视程度。在传统的数据合作中，通常采用数据脱敏的方式将一方数据给到另一方，并由其进行本地建模。虽然数据脱敏方案实现了一定程度的隐私保护，但仍然能通过收集到的相关数据，损害数据方的利益，甚至侵害客户的个人隐私。此外，经过脱敏处理的数据可用性会受到严重影响。在数据合作之前，传统方案需要通过比较哈希值的方式进行撞库，这样一方就会留存大量的哈希值造成对方客户名单的泄露。

隐私保护计算为金融机构间，甚至跨行业的数据合作、共享提供可能。PSI 技术可以解决数据对齐时造成客户名单泄露的问题，联邦学习可以保证各方数据不出本地的情况下实现联合建模、预测等。

图 15 为金融领域中反欺诈联邦学习建模的落地应用。一般情况下，单一机构自有数据量小，建模样本数不足，可以联合多家机构的数据进行联合建模。当一家银行获得和新型欺诈行为相关的数据时，可以及时更新反欺诈模型，使其他银行也能够快速具备预测和识别新型欺诈行为的能力，提高整个银行业的反欺诈水平。

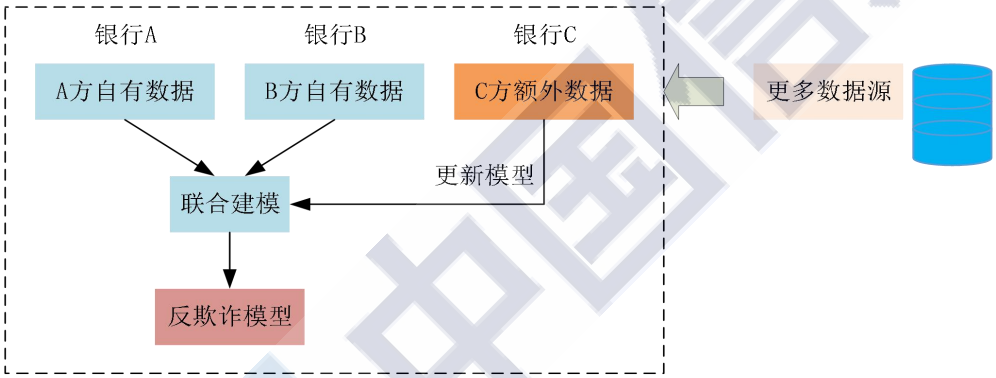


图 15　反欺诈联邦学习示意图

（二）政务领域

在国家积极推动政企数据融合、数据生产要素化的大方向下，各地政府积极建立政务数据开放平台、大数据中心，致力于服务各行各业。政务数据通常涉及社保数据、公积金数据、税务数据、生活数据、交通数据等。但是这些数据属于不同部门，“数据孤岛”情况严重，想要共享这些数据存在协调困难、审批手续繁杂等问题。同时这些数据涉及大量公民隐私，管控更加严格，进一步阻碍政务数据在部门之间、政企之间的合作。

通过隐私保护计算和其他技术的结合，可以有效保护各部门的数据，在一定程度上解决政务“数据孤岛”问题，提高政府治理能力。例如通过视频、位置、交通等多部门数据对治安防控、突发事件进行研判，合理调配资源，提高应急处理能力和安全防范能力。此外，还可以联合多部门的数据对道路交通状况进行预判，实现车辆路线最优规划，减缓交通拥堵。

以疑犯信息查询为例（如图 16 所示），假设公安机关有一份疑犯名单，需要到其他部门查询疑犯的相关信息，但是“疑犯”这个身份信息对个人而言比较敏感。利用隐私查询技术，在查询疑犯相关信息的同时，公安机关不需要跟其他部门共享疑犯名单，保护疑犯隐私。

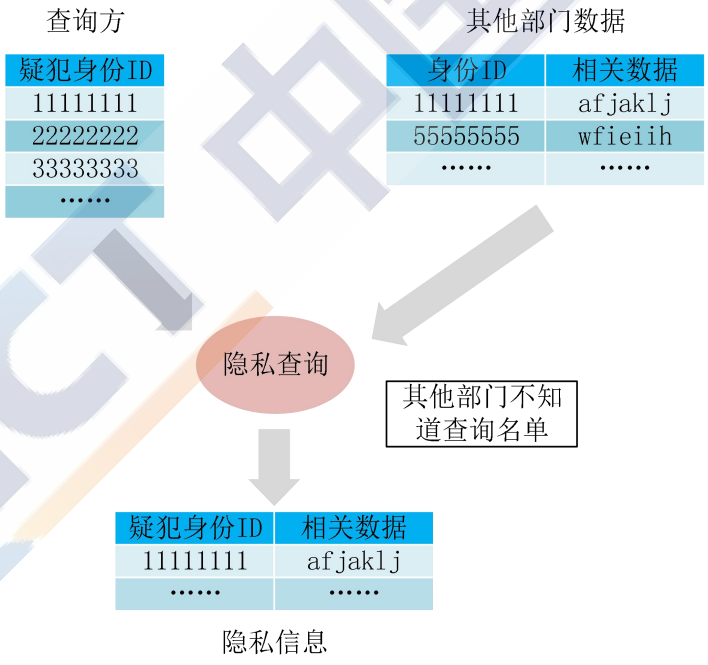


图 16　疑犯信息查询示意图

（三）医疗领域

随着互联网以及电子病历的大量普及，各家医疗机构积累了大量

的医疗数据，这些数据对于病人来说是极其敏感的。随着人工智能和医疗的紧密结合，越来越多的个人数据被用于临床诊断、医学研究、公共健康等各个方面，这就增加数据泄露的可能性。

想要使用人工智能对某一疾病进行早期发现或临床诊断，一方面需要收集不同维度的数据包括临床数据、基因数据、化验数据等，另一方面也需要收集来自不同群体、不同地区的样本数据，单个医疗机构无法积累足够的数据来进行模型训练。通过隐私保护计算，可以对不同的数据源进行横向和纵向的联合建模，保证各方医疗数据安全。另外，对于 DNA 测试，用户可以通过 PSI 等技术将某段 DNA 序列和数据库进行匹配，实现遗传疾病诊断。

举例来说[43]。为了应对新冠肺炎疫情带来的医疗挑战，医疗机构需要在全球范围内共享新冠肺炎疫情数据。如通过人工智能识别肺部 X 光图像来诊断新冠肺炎。各医疗机构先在本地建立模型，再通过 SMPC 等技术联合其他医疗机构更新模型参数，在保护各方数据隐私安全前提下，提高图像模型诊断能力。

[43] Ulhaq A, Oliver B. COVID-19 imaging data privacy by federated learning design: A theoretical framework. arXiv preprint arXiv:2010.06177 (2020)

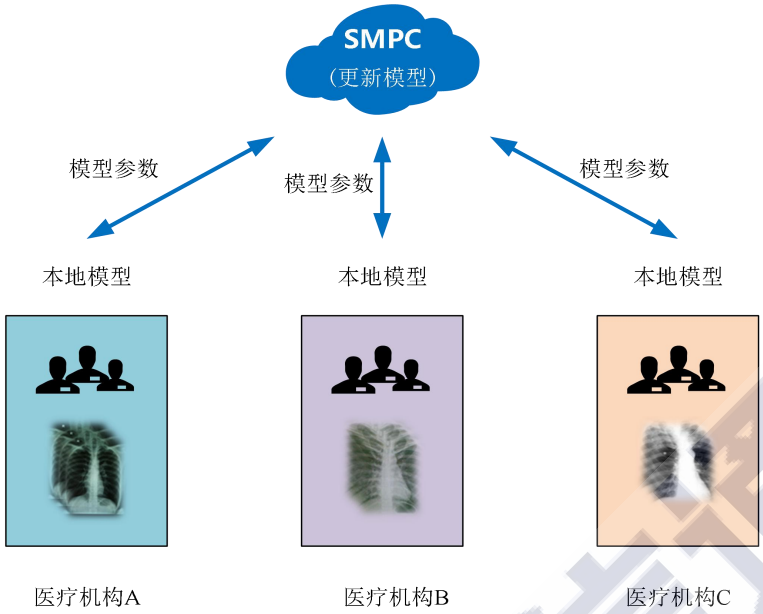


图 17　新冠人工智能联合诊断示意图

五、隐私保护计算发展展望

隐私保护计算作为平衡数据价值挖掘和隐私保护有效解决方式，为数据流通和价值共享提供了一条重要的技术路径，引起了产业内外的广泛关注。然而，隐私保护计算在技术实现、公众信任建立、应用推广等方面仍然存在诸多挑战。因此，隐私保护计算技术的发展，仍然需要各方协同精诚协作，继续努力。

一是合规驱动，拓展发展空间。当前，隐私保护已成为全球共识，《中华人民共和国网络安全法》《中华人民共和国密码法》《数据安全法（草案）》《个人信息保护法（草案）》等系列政策法规陆续出台，隐私保护的必要性和紧迫性不言而喻。**一方面**对于促进公众隐私保护意识觉醒，维护数据权利主体的合法权益提供了有力的法律保障。**另一方面**随着顶层设计的不断优化完善，数据安全和隐私保护合规要求将进一步明确，在数据要素经济价值挖掘和新基建大数据中心建设

发展的牵引下，隐私保护计算应用场景将进一步拓展，隐藏的巨大市场潜能有望被进一步激发。

二是标准引领，凝聚行业共识。虽然隐私保护计算目前尚处在发展初期，但在当前打破“数据孤岛”，增进数据协同价值挖掘的需求日益迫切的大背景下，亟待凝聚各方共识。以标准化形式将隐私保护计算关键技术的探索与实践中积累的宝贵经验进行固化，以此指导隐私保护计算技术的构建部署，纾解重复投入、建设分散等问题，充分发挥隐私保护计算技术落地应用的标准引领和支撑作用。

三是需求牵引，提升技术成熟度。虽然针对隐私保护计算的关键技术研究已开展多年，但在规模化应用时仍然存在多项难点，如应用性能瓶颈、安全性证明、数据质量规范性差等问题。当前市场对于隐私计算产品及服务的选择是建立在对于以市场落地实际需求为牵引的前提下，需产学研用协同，不断夯实关于安全多方计算、联邦学习、差分隐私等理论研究基础，积极开展面向实际产业需求的工程探索，不断提升隐私保护计算的技术成熟度和产业化能力。

四是多方协同，弥合信任鸿沟。隐私保护计算技术原理复杂难于理解、试错成本高，不可避免要经历“质疑”到“追捧”再到“理性”的这样一个过程。隐私保护计算当前正处在发展期望膨胀期，但迅猛发展的市场也极易出现解决方案隐私保护水平高低不均、落地效果良莠不齐的现象。如何提升公众对隐私保护计算技术的认知程度，防止行业疑虑蔓延，弥合公众对隐私保护计算技术的信任鸿沟，亟待建立科学、严谨的隐私保护计算技术产品和解决方案的评估机制，开展专

业的技术检测和效果评估，提高隐私保护计算技术的公信力，共同保障隐私保护计算技术产业应用的健康发展。

CAICT 中国信通院

附录一：缩略语对照表

术语	缩略语
联邦学习 （Federated Learning）	FL
安全多方计算 （Secure Multi-Party Computation）	SMPC
秘密共享 （Secret Sharing）	SS
不经意传输 （Oblivious Transfer）	OT
混淆电路 （Garbled Circuit）	GC
隐私集合求交 （Private Set Intersection）	PSI
隐私信息检索 （Privacy Preserving Information Retrieval）	PIR
可信执行环境 （Trusted Execution Environment）	TEE
差分隐私 （Differential Privacy）	DP
本地差分隐私 （Local Differential Privacy）	LDP

CAICT 中国信通院

部分同态加密方案 （Somewhat Homomorphic Encryption）	SHE
全同态加密方案 （Fully Homomorphic Encryption）	FHE

CAICT 中国信通院

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62304364

传真：010-62304364

网址：www.caict.ac.cn