OPEN MPC

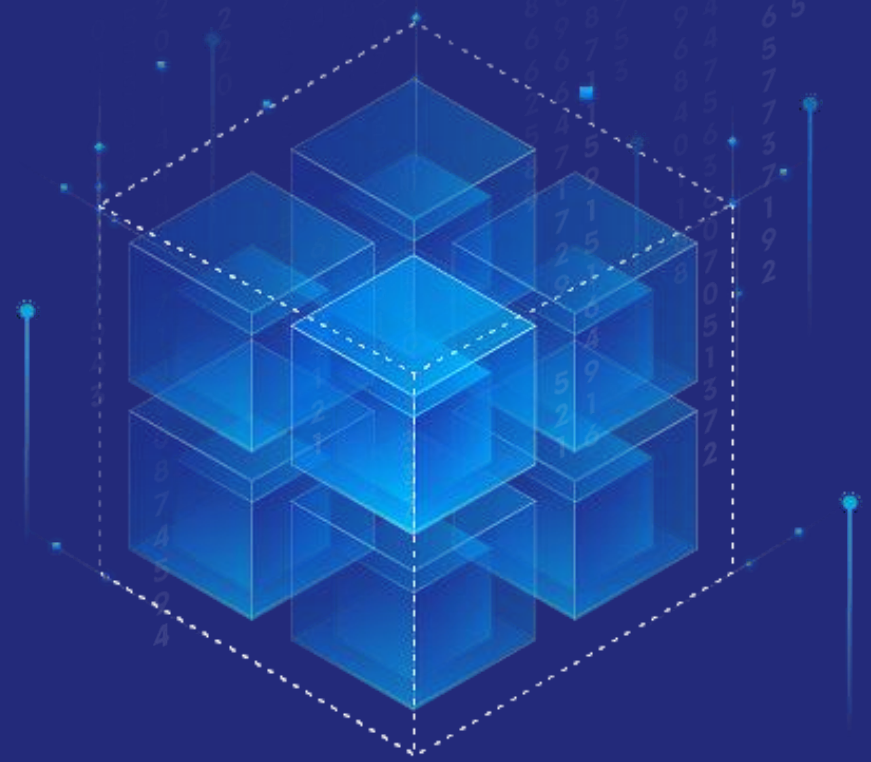
2023全球隐私计算报告

杭州数据协同创新未来实验中心 · 隐私计算联合创新实验室

2023年11月

版权声明

组织单位



指导单位

- 杭州数据资源管理局

联合发起单位

- 火山引擎
- 联通研究院
- 数据要素社
- 隐私计算联合创新实验室
- 杭州数据交易所
- OpenMPC社区
- 西安交通大学
- 中国电信翼支付

支持单位

- 杭州数据安全联盟
- 杭州国际数字交易联盟

（排名不分先后，以拼音首字母排序）

编写成员

主编：

熊婷

编写组成员：

陈孔阳、何志坚、姜亚彤、林浩、路航、李增鹏、李雪雁、李安国、柳兴、梁栋、庞雷、潘凯伟、任雪斌、史楠迪、WenHui Zhang、王凯崙、由林麟、杨树森、张锦锋、周旦

（排名不分先后，以拼音首字母排序）

OPEN MPC

CONTENTS

目录

01

第一章：

全球隐私计算发展概览

政策法规动态-国内

2023年3月7日

根据国务院关于提请审议国务院机构改革方案的议案，组建国家数据局。

2023年年10月25日

国家数据局挂牌成立。

2023年11月10日

国家数据局局长刘烈宏在北京数据基础制度先行区启动活动上表示我们正要积极推进隐私计算、数据空间、区块链等数据流通技术研发和集成应用，布局建设数据基础设施，为数据可信、高效流通提供有力的基础支撑。

数据共享方面

2023年2月27日 中共中央 国务院印发《数字中国建设整体布局规划》。《规划》提出，到2025年，数字基础设施高效联通，数据资源规模和质量加快提升，数据要素价值有效释放。

2023年7月30日 国务院办公厅关于印发《政务服务电子文件归档和电子档案管理办法》，指出各级政务服务机构应当在符合国家有关法律法规要求的前提下，依托政务服务平台积极推进本单位政务服务电子文件和电子档案共享利用。

数据使用保护方面

2023年3月7日 根据国务院关于提请审议国务院机构改革方案的议案，组建国家数据局。负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等，由国家发展和改革委员会管理。10月25日，国家数据局挂牌成立。

2023年8月3日 国家网信办发布《个人信息保护合规审计管理办法（征求意见稿）》，指出专业机构应当采取相应技术措施和其他必要措施，保障数据安全。

2023年8月8日 国家网信办发布《人脸识别技术应用安全管理规定（试行）（征求意见稿）》，面向社会公众提供人脸识别技术服务的相关技术系统应符合网络安全等级保护第三级以上保护要求，并采取数据加密等措施保护人脸信息安全。

2023年8月25日 国家金融监管总局、中国人民银行、中国证监会、国家网信办、国家外汇管理局《关于规范货币经纪公司数据服务有关事项的通知》，构建覆盖数据全生命周期和应用场景的安全保护机制,开展数据安全风险监测评估。

隐私计算方面

2023年1月3日 工信部等16部门发布《关于促进数据安全产业发展的指导意见》，指出优化升级数据识别、分类分级、数据脱敏、数据权限管理等共性基础技术，加强隐私计算、数据流转分析等关键技术攻关。加强数据质量评估、隐私计算等产品研发。推进安全多方计算、联邦学习、全同态加密等数据开发利用支撑技术的部署应用。

2023年5月22日 工信部发布《工业领域数据安全标准体系建设指南（2023版）（征求意见稿）》，提出将多方安全计算、联邦学习等作为数据共享安全技术产品标准重点建设方向，将数据脱敏、可信执行环境等作为数据安全防护技术产品标准重点建设方向。

2023年7月24日 央行发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》，指出数据处理者采用隐私计算等技术促进数据融合创新应用时，应当确认原始数据未离开自身控制范围，且多个数据提供行为关联后，暴露约定范围外信息的风险可控。采用隐私计算技术提供数据时，应当建立统一的技术风险评估和控制策略，明确安全可验证性、性能可接受性等风险对应的缓释措施。

政策法规动态-国外

英国皇家学会发布隐私增强技术报告（ From privacy to partnership ）。报告发现人们对隐私增强技术的信任度仍然很低，这意味着它们提供的协作和分析潜力并未被开发。

2023年1月

联合国大数据和数据科学专家委员（UNCEBD）会发布《隐私增强技术指南》（The PET Guide），重点关注隐私增强技术在官方统计数据中的应用，旨在帮助各国的国家统计局更好地理解和运用隐私增强技术处理敏感数据。

2023年2月

经济合作与发展组织（OECD）发布《新兴隐私增强技术：成熟度、机遇和挑战报告》，重点关注隐私增强技术工具的优势。

2023年3月

英国金融行为监管局（FCA）发布了有关新兴技术（EmTech）研究中心的信息，其中合成数据和隐私增强技术是重点领域。

2023年3月

美国白宫科技政策办公室（OSTP）发布《促进数据共享与分析中的隐私保护国家战略》，支持利用隐私增强技术进行数据分析、获取数据价值，同时确保用户隐私、秘密安全。

2023年3月

G7七国集团数据保护和隐私机构（DPA）在日本举行会议，批准了 “三支柱计划”，包括开发和实施信任数据自由流动（DFFT）概念、新兴技术和加强执法合作，并就隐私增强技术进行了讨论。

2023年6月

2023新技术热点

AIGC技术发展带来的影响

- 在推动数实结合、加快产业升级的进程中，金融、医疗、制造、工业等各行各业AIGC应用也都在快速发展。
- AIGC的应用在推动产业发展的同时，也带来了数据泄露的风险。AIGC的应用是借助大模型厂商提供的服务进行的，存在着模型和数据隐私泄露风险。
- 如何通过异构 AI 隐私计算的技术手段，保护大模型在训练、部署和服务时的数据和模型参数安全，满足 AI 大模型应用落地过程中的隐私保护需求。
- 如何利用AI的生成式能力助力隐私计算的发展，给隐私计算带来了新的挑战。

区块链技术发展带来的影响

- 在隐私计算中，数据共享缺乏安全性校验，参与者身份及数据缺乏记录和验证；数据共享参与者缺乏合理的激励机制和公平的协作环境。
- 区块链技术可以解决隐私计算中参与者身份与数据的可信验证问题，可以提供公平合理的合作环境。
- 隐私计算技术和区块链技术结合可以提高隐私计算中身份认证及密钥管理的安全性和灵活性、解决数据共享参与者身份及数据可信问题、增强区块链的隐私保护能力。

云原生技术发展带来的影响

- 云 MaaS理念提出以智能模型为核心的开发范式，搭建了智能云计算技术和服务架构提供包括模型训练、推理、部署、精调、测评、产品化落地等在内的全方位服务。
- 云原生在企业中的应用越来越广泛和深入，如果隐私保护不到位，云原生技术的发展会带来巨大的隐私泄露问题。
- 针对云原生网络架构虚拟化、连接情况复杂、网络边界动态变化的特点，将模型作为一种服务提供给用户，需要实现对用户数据要素的隐私保护和对模型参数本身的隐私保护，想要推动云原生技术的发展和完善，离不开隐私计算技术的护航。

量子计算技术发展带来的影响

- 量子计算可在较短的时间内破解传统加密算法，给基于密码学原语的隐私计算长效安全性带来威胁，如何实现抗量子是量子时代隐私计算面临的巨大挑战。
- NIST已广泛征集关于后量子密码算法的研究，将后量子密码算法迁移到隐私计算的组件中可以应对量子计算对目前隐私的威胁。
- 量子密钥分发也是应对量子计算威胁的手段之一。量子密钥分发可用于传输隐私信息，保证数据要素安全，完善隐私计算中数据出域的信任链问题，从而推动抗量子隐私计算的发展。

2023隐私计算行业国际动态

- 隐私增强技术（PET）发展势头强劲，获得政府、公共机构、监管机构、企业的广泛关注；
- PET逐步走向立法和监管变革，诸如英国ICO指南草案、加拿大C-27隐私法、拟议的欧盟人工智能法案、美国人工智能权利法案；
- PET技术标准和质量评估措施迅速发展，即将推动公共和私营部门机构的PET应用案例建设。

国际组织	行业事态
经济合作与发展组织 (OECD)	发布《新兴隐私增强技术：成熟度、机遇和挑战》，重点关注隐私增强技术（PET）
英国ICO PET 指南草案	提出企业的合法数据共享方法，例如同态加密、安全多方计算、联邦学习、可信执行环境、委知识证明、差分隐私、合成数据
英国金融行为监管局 (FCA)	重点关注的新兴技术：合成数据、PET
英国皇家学会&艾伦图灵研究所	需要权衡PET的数据治理和数据隐私
美国科学技术政策办公室(OSTP)	提出《推进隐私保护数据共享和分析国家战路》(PPDSA)，支持 PPDSA 技术和方法 “以公平的方式最大化其利益、促进信任并降低风险”
英国&美国	建立数据桥梁，使个人数据在两个国家之间自由流动，无需进行传输影响评估
加拿大隐私专员办公室 (OPC)	更新加拿大联邦私营部门隐私法(Bill C-27），提出合成数据的去识别化，将去识别化数据仍视为个人信息
联合国	发布《联合国官方统计隐私增强技术指南》，帮助各国统计局在处理敏感数据时使用PET
土耳其	监管机构需要协助企业负责任地开发和部署PET，平衡PET的技术推广与监督监管，以保护个人隐私
欧盟-美国贸易和技术理事会(TTC)	发布《可信人工智能和风险管理评估和测量工具联合路线图》，开发人工智能风险管理和可信人工智能工具、方法和途径
英美隐私增强技术挑战赛	英国和美国政府发起一系列有奖挑战，使用合成数据开发保护隐私的联合学习解决方案，奖金池为130万英镑，挑战一利用综合全球交易数据打击国际洗钱，挑战二利用综合健康数据应对大流行

关键词热度分析


数据共享
差分隐私
隐私保护
数据交易
同态加密
电力
大数据
量子计算
隐私计算
金融
Pets
元宇宙
智能制造
全同态加密
可信数据协作
供应链
国产替代
隐私计算一体机
数据合规
联邦学习
政务
数据交易所
密码学
数据经纪
零知识证明
医疗
数据确权
Aigc
可信执行环境
安全多方计算
安全性
数据安全
数据清洗
合成数据
机密计算
性能
营销广告
数据泄露
区块链
人工智能
开源
数据跨境
数据清洁室
公共数据
隐私增强技术
数据要素
大模型
信息安全

02

第二章：

2023全球隐私计算图谱

隐私计算图谱2023

产品/技术需求方

政府侧

国家税务总局 State Taxation Administration
中华人民共和国公安部 The Ministry of Public Security of the People's Republic of China

数据交易所

贵阳大数据交易所
北京国际大数据交易所 Beijing International Data Exchange

金融

中国光大银行 China Everbright Bank
交通银行 Bank of Communications
WeBank 微众银行
中国农业银行 Agricultural Bank of China
WeBank 微众银行
泰康人寿 Taikang Life
浦发银行 SPD BANK
中国工商银行 Industrial and Commercial Bank of China
中国人寿 China Life
招商银行 China Merchants Bank
中国银联 China Unionpay

通信

中国移动 China Mobile
中国联通
中国电信 China Telecom

医疗

美年大健康 Health 100

其他

中国民航 CAAC
国家电网 State Grid

新生态

确权机构

北京市知识产权局
浙江省数据知识产权登记平台
SAG 温州数安港 WEN ZHOU SHU AN GAN
人民数据

评估机构

CEA
上海东洲资产评估有限公司 SHANGHAI ORIENT APPRAISAL CO., LTD.

咨询机构

Deloitte. 德勤
EY 安永
KPMG
pwc

安全合规

环球律师事务所 GLOBAL LAW OFFICE
中伦律师事务所 ZHONG LUN LAW FIRM
汇业律师事务所 HUI YE LAW FIRM

经纪服务商

广东电网 能源投资有限公司
广州金控 征信服务有限公司
唯品会 vipshop.com

产品/技术提供方

综合服务商

蚂蚁集团 ANT GROUP
HUAWEI
Tencent 腾讯
Baidu 百度
中国移动 China Mobile 5G
京东
字节跳动 ByteDance
天翼数科 Digital Technology
Google
安恒信息 DAS-SECURITY
Meta
SAMSUNG
IBM
Microsoft
联通数科 Unicom Digital Tech

专精服务商

华控清交 TSINGJIAO INFORMATION SCIENCE
BaseBit.ai 翼方健数
洞见科技 INSIGHTONE
原语科技 PRIMITIVE HUB
蓝象智联
锘崴科技 NYXCLOUDS TECH
数牍 sudo
富数 FUDATA.CN
同态科技 TONGTAI
煌辰数智 STOACACO
冲量在线 IMPULSEONLINE
融安数科 RONGANDIGITECH
同盾科技 www.tongdun.cn
TASS 江南天安
CLUSTAR 星云
seceum
ZAMA
baffle
SEATA
sharemind by CYBERNETICA
OpenMined
Cape Privacy
unbound security

开源产品

Syft
PRIMIHUB
SECRET FLOW 隐语
FATE
FedML
[M]S 昇思 MindSpore
TFEncrypted
EMP
Rosetta
MesaTEE
Occlum
Hehub
Microsoft SEAL

隐私计算+

区块链

趣链科技 HYPERCHAIN
云象 YUNPHANT
熠智科技 YeeZTech
零数科技 LINGSHU.NET
八分量
数秦科技 DataGm.com
成都链安 BEOSIN

AIGC

文心大模型
腾讯混元
通义
火山引擎
科大讯飞 IFLYTEK
讯飞星火
日日新 sensenova
OpenAI
LLAMA

元宇宙

iOS
Meta
COL 中文在线
KUNLUN
miHoYo
Goertek
bilibili
htc

信息安全

NSFOCUS 绿盟科技
YASO
安恒信息 DAS-SECURITY
360
H3C 数字化解决方案领导者

大数据

Fongwell
芥禾数据
微言科技
Ultrapower 神州泰岳
TRANSWARP 星环科技
聚合数据
inspur 浪潮

研究机构

ICT
浙江大学 ZHEJIANG UNIVERSITY
复旦大学 FUDAN UNIVERSITY 1905
广州大学 GUANGZHOU UNIVERSITY
南京大学 NANJING UNIVERSITY 1902
北京航空航天大学 BEIHANG UNIVERSITY
上海交通大学 SHANGHAI JIAO TONG UNIVERSITY
Berkeley UNIVERSITY OF CALIFORNIA
Northwestern University
TECHNISCHE UNIVERSITÄT DARMSTADT

标准机构

全国信息技术标准化网 China National Information Technology Standardization Network
工业和信息化部电子工业标准化研究院 中国电子技术标准化研究院
CAICT 中国信通院

硬件厂商

HUAWEI
HYGON 中科海光
Phytium 飞腾
兆芯
沐创集成电路
ARM
intel
NVIDIA
AMD

垂直媒体

隐私计算社区 OPEN MPC

03

第三章：

全球隐私计算技术进展

安全多方计算

密码学原语研究：
更注重效率与安全

- 聚焦提升协议执行效率
  - 同态秘密共享（HSS，Homomorphic Secret Sharing）因其可行性和效率优势而成为全同态加密（FHE，Fully Homomorphic Encryption）的另一替代方案。
- 聚集于提升协议的安全性
  - Derandomizable FSS 实现了能够抵抗恶意攻击者的saPSI（Structure-Aware Private Set Intersection）协议。

从计算到学习：
与机器学习广泛融合

- 融合深度学习，利用混淆电路协议对分布式客户端生成的数据进行扩展的深度学习分析。
- 融合迁移学习，通过部署与数据无关的特征提取方法，在不泄露任何关于私有图像或分类器的信息的情况下，实现图片分类。
- 融合知识图谱，实现保护用户数据的推荐。

从理论到实践：
更多实用框架提出

- Sequre：安全多方计算在生物信息领域的最新开源框架，已应用与在各种生物信息学任务上，包括全基因组关联研究、药物-靶标相互作用推断等。
- Squirrel：摩根大通服务金融行业的安全多方计算框架（未开源），可在纵向切分的数据集上进行安全的两方GBDT训练，训练过程中不会泄露任何敏感的中间信息。

联邦学习

- 目前联邦学习技术除了支撑主流的机器学习方法和模型训练外，更多聚焦于安全与隐私保护技术上， 可信联邦学习成为重要趋势，联邦大模型技术、模型产权保护（IPR）、模型定价等正在初步探索，在应用方面则突出了物联网、区块链移动设备方面的研究。

公平性

为避免模型偏差所造成的影响，联邦学习对数据集精度要求与日俱增，许多研究团队着力探讨开放训练的公平性问题，通过定义公平性衡量指标，来保证联邦参与者的贡献与收获均衡，并实现每一个参与者的持续激励。

安全性

除了传统隐私性的考虑，联邦学习作为分布式系统也容易受到恶意攻击，如1）通过获取训练过程中的中间参数，逆向推理得到隐私数据，2）通过数据投毒，干扰联邦学习过程，导致模型训练失效。通过研究相关的防护机制，保证联邦学习的安全性。

大模型

通过分布式的算力与数据实现大模型的联邦化训练、微调与部署。为适配异构的算力与数据，实现大模型在资源受限条件下的有效训练，通过大小模型的有效联动，实现本地小模型的高效训练、全局大模型的精准更新，以及更新模型的个性化部署。

新模式

基于去中心的联邦学习过程，可对现有的AI模型与学习方法进行联邦化、隐私化改造，如联邦图学习、联邦强化学习、联邦元学习等。同时，针对实现应用场景，如物联网应用，随着用户与内容的日益丰富，增量式联邦学习成为支持相关服务与应用的基础。

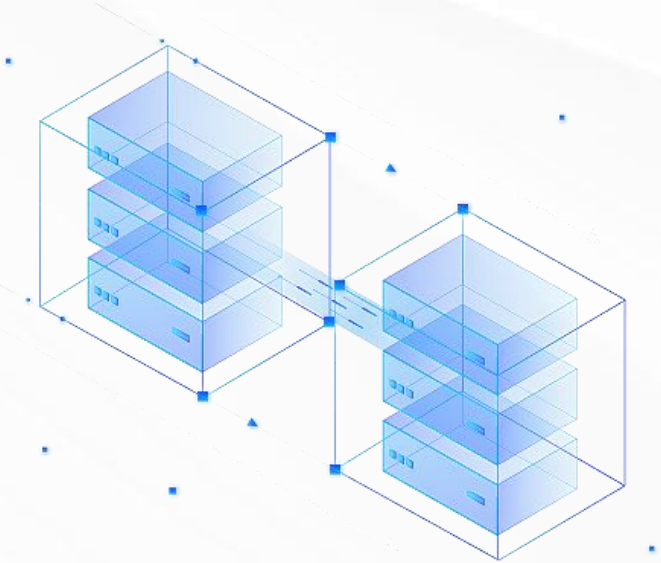
可信执行环境

- 随着越来越多的业务上云，端到端的全链路可信或机密正在慢慢成为公有云基础设施的默认要求而不再是一个特性，需要综合利用加密存储、安全网络传输、机密计算来实现对用户敏感数据全生命周期的保护。机密计算是当前业界正在补齐的环节，主流的硬件平台已经部分提供或正在实现对机密计算的支持，目前主要云厂商(Azure , AWS, GCP 等）的机密计算架构产品如下图所示，正在如火如荼的升级支持中。其中AWS坚持走自己的路线、没与具体硬件绑。 2023年，我们看到Google拥抱AMD SEV系列云产品，并发布了Intel TDX VM 的预览版本。Azure还在2023年率先推出了对GPU TEE （StrongBox，Graviton， H100）的支持。阿里云拥抱新产品，支持了TDX VM，并率先提出用TDX保护大模型的解决方案。

企业名单 / TEE产品	机密虚拟机	GPU 机密虚拟机	机密容器	机密数据库	机密机器学习平台
AWS	AWS 有全栈自研的 Nitro Enclaves 机密虚拟机，和基于AMD的SEV-SNP机密虚拟机	AWS目前无此类产品	AWS目前无此类产品	AWS Clean Rooms提供机密计算下的多用户数据查询	DEeep AWS Learning Container
Azure	Azure 有支持SEV，SEV-SNP，TDX的虚拟机	Azure有GPU Nvidia TEE，推出两个型号 Ampere 100+SGX，H100+SEV-SNP	Azure Kubernetes Service (AKS) 和SCONE, Fortanix, Anjuna 一起提供Confidential Containers 产品， 包括基于SGX SDK/Openenclave的Enclave-aware containers； AKS同时也支持基于 SEV-SNP 的安全容器	Azure 有基于SEV的Always Encrypted with secure enclaves in Azure SQL Database， 和基于SGX的MySQL DB， 还有和blockchain 结合的Azure Confidential Ledger 产品	Azure有 Confidential Inferencing ONNX Runtime
Alibaba Cloud	阿里云已有全栈自研 阿里云虚拟化Enclave （基于第三代神龙架构）和 基于SGX, TDX, SEV 的机密虚拟机	阿里云和冲量在线等，一起推出GPU机密虚拟机互联互通系统	阿里有 ACK-TEE 1.1 和 KubeTEE (link, link)做机密容器调度，有安全沙箱 (轻量级虚拟化) 和 Inclavare Containers 等机密容器运行时。	阿里云全加密数据库， 使用SGX支持RDS PostgreSQL实例； 阿里云也有基于TDX的全密态数据库	DataTrust隐私增强计算平台，并推出机密计算保护大模型 等解决方案
Google Cloud	GCP 推出了基于SEV， SEV-SNP 和 TDX 的Confidential VM， 它的disk用Split-Trust Encryption Tool做云盘加密	GCP 推出了基于SEV-SNP 和 TDX 的H100 Confidential VM	GCP推出了基于SEV和SEV-SNP 的Container (Confidential GKE Nodes)	Dataflow 提供内嵌内存加密的SEV机密虚拟机来处理数据流水线	机密 Dataproc 通过全代管式 Spark、Hadoop 以及其他开源工具和框架实现大数据处理

差分隐私

- 差分隐私能够解决传统隐私保护的两个关键问题。首先，在最大背景知识假设下，差分隐私保护无需考虑攻击者所拥有的任何可能的背景知识。其次，差分隐私对隐私保护进行了严格的定义并提供了量化评估方法，使得不同参数处理下的数据集所提供的隐私保护水平具有可比较性。因此，差分隐私理论迅速被业界认可，并逐渐成为隐私保护领域的一个研究热点。



中心化差分隐私

中心化差分隐私研究已较为广泛，传统主要集中在统计分析和机器学习/深度学习模型训练场景，当前研究最新进展已开始尝试将差分隐私引入到自然语言处理、生成式模型、视频数据分析等复杂应用场景中。

本地化差分隐私

本地化差分隐私由于适用于大规模环境部署，受到工业界的广泛应用。当前研究进展主要集中于实现更多复杂场景的数据分析算法设计。一方面，针对统计查询场景，主要集中在对高维、流式、图数据等统计分析场景算法的优化；另一方面，针对机器学习与深度学习场景，主要集中在与深度学习、联邦学习的结合，近来也开始实现与大语言模型结合，实现大语言模型预训练与推理过程的本地隐私保护。

分布式差分隐私

中心化差分隐私对可信假设要求较高但能够保持较好数据分析效用；而本地化差分隐私对可信假设要求较低但相比中心化差分隐私的分析效用较低；分布式差分隐私通过结合一些密码学原语辅助的安全性，可以实现分布式隐私保护的同时获得接近中心化差分隐私的效用性。

混洗差分隐私

混洗差分隐私通过第三方的消息混洗节点，实现本地差分隐私消息收集过程的匿名性，通过增大隐私安全特性来降低所需的噪声，从而提升数据效用性，也收到当前理论研究的关注。作为分布式差分隐私的一种变体，近来也被广泛应用到联邦学习算法的设计中。

隐私放大理论

近来的研究集中在如何结合算法设计中采样、压缩、内在随机性等特性实现无需额外噪声的隐私放大。

同态加密

理论优化

底层优化

- 小模量格密码
- 重线性技术
- 代数密码构造
- 快速自举
- 矩阵旋转
- CRT Batching，RNS

功能增强

- 密态结果可验证
- 高效密态搜索
- 误差权衡控制
- 多方计算支持
- 多协议密文转化
- 密态算子轻量

性能优化

- 存储开销降低
- 高效AI密态算子
- 提升计算速度
- 多协议混合优化
- 新的同态结构
- 基础算子优化

应用探索

应用创新

- 神经网络、联邦学习、安全多方计算
- 隐私集合求交、隐匿查询、门限签名
- 密文数据库、协同过滤

硬件辅助计算

- ASIC、FPGA、GPU、CPU
- Cuda架构、AVX2指令集等
- FTT，NTT，iNTT的并行化

降低开发成本

- 更加高效自动化的同态编译

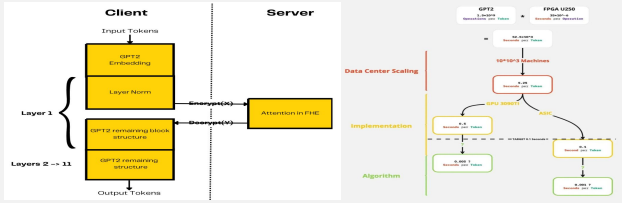
ZAMA Concrete

fully-homomorphic-encryption

行业落地

跨境数据流通

自然语言大模型隐私推理



船舶隐私维护检测

技术合规政策

2023年2月3日，国家互联网信息办公室发布《个人信息出境标准合同办法》，指出境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全。

2023年6月1日，外交部发布《中国关于全球数字治理有关问题的立场》，指出促进数据依法有序自由流动。国家间缔结跨境调取数据双边协议，不得侵犯第三国司法主权和数据安全。

2023年8月13日，国务院印发《关于进一步优化外商投资环境加大吸引外商投资力度的意见》，明确探索便利化的数据跨境流动安全管理机制，包括高效开展重要数据和个人信息出境安全评估，促进数据安全有序自由流动。

2023年9月28日，国家互联网信息办公室发布《规范和促进数据跨境流动规定（征求意见稿）》，规定数据处理者向境外提供重要数据和个人信息，应当遵守法律法规和相关义务。

2023年5月30日，国家互联网信息办公室发布《个人信息出境标准合同备案指南（第一版）》，指出尽合理地努力确保境外接收方采取技术和管理措施。

2023年6月29日，国家互联网信息办公室与香港特区政府创新科技及工业局签署《关于促进粤港澳大湾区数据跨境流动的合作备忘录》，建立粤港澳大湾区数据跨境流动安全规则。

2023年7月10日，欧盟委员会通过“欧盟-美国数据隐私框架”的充分性决定，框架引入了新的具有约束力的保障措施，美国将确保对从欧盟传输到美国公司的个人数据提供与欧盟的保护水平相的保护。

2023年9月21日，英国确认“英美数据桥”（UK-US data bridge）于10月21日生效，将允许组织通过“欧盟-美国隐私框架的英国扩展”进行美英间数据跨境传输。2023年6月9日，英美发布声明，承诺建立“数据桥”。

2023年9月9日，英国政府发布声明称英国与新加坡签署一项新战略合作伙伴关系协议，将加强双方在安全、科技创新和研发方面的共同合作，包括双方探索促进跨境数据流动机制。

2023年9月3日，东盟启动《数字经济框架协定》（DEFA）谈判工作，以促进东盟成员国密切合作，创建可持续和包容性的数字生态系统。重点关注数字贸易、跨境电商、网络安全、数据跨境流通等新兴议题。

2023年8月15日，巴西数据保护局发布《个人数据国际传输条例》草案，规定巴西数据保护局将确定满足数据跨境条件的国家或地区名单，以允许个人数据在巴西与这些国家或地区之间自由流动。

技术合规挑战

数据源的合规性问题

“脏数据”或“毒数据”将带来“数据投毒”风险，导致计算结果不准确，甚至可能泄露其它合法数据信息。此外，数据来源如果不合法，在隐私计算后期使用中将面临侵权责任。数据源的合规性将成为重点解决的问题之一。

隐私计算是否等同匿名化问题

已经匿名化的信息可以不受相关法律法规的约束。由于技术操作过程的各个节点以及个人信息的存储、传输过程难以完全做到无法反推、不会泄露等，且隐私计算无法保证完全或者绝对的匿名化。隐私计算需要根据相关法规标准进行技术合规性审查。

使用隐私计算是否正当、必要和诚信问题

《个人信息保护法》规定，处理个人信息应当遵循合法、正当、必要和诚信原则。在某些隐私计算应用场景中，可能必要性不足，正当性不足，或者有违诚信。

隐私计算技术的合法性授权问题

隐私计算可能涉及到诸多主体参与到代码的开发、模型的建立以及模型的测试等环节，其中知识产权的归属、授权使用的范围、授权链的完整性以及各自在隐私计算中权利义务的分配，均需要仔细分析。

隐私计算技术的安全性和效率合规问题

通过基于密码学的技术路线开发的相关产品，实际使用中的安全性难以验证。当前隐私计算技术处理的数据规模并不是很大，部分产品计算效率尚未符合实际使用需求，安全性和效率合规方面亟需完善。

数据跨境流动问题

参与数据跨境流动的国家需要基于数据跨境相关协议，包括数据跨境传输路径的规则、标准合同、约束性企业规则、数据隐私保护规则等合法进行数据跨境流动，不仅仅基于某一国家或地区数据保护相关法规政策。隐私计算技术的发展和产品的推广需要同时研判各国数据管理法规及法律环境和相关数据隐私框架要求，针对性建立隐私计算技术和产品认证体系，确保相关技术和产品符合数据跨境传输合规认证。

互联互通标准体系

- 逐步构建完善的互联互通标准体系。打造兼容性好，开放性高的互联互通协议，加速数据安全流通。

全球首个隐私计算互联互通国际标准

IEEE SA全球首个隐私计算互联互通标准《Interworking Framework for Privacy-Preserving Computation》由洞见科技2022年6月牵头编制，旨在建立隐私计算互联互通技术框架规范，该标准正在制定中。

首个国家标准

隐私计算互联互通国家标准《隐私保护的数据互联互通协议规范》由富数科技2021年8月牵头立项，该规范确立了完整隐私计算互联互通研究内容总框架，该标准仍正在制定中。

通信行业系列规范

《隐私计算 跨平台互联互通》系列标准由中国信通院牵头编制，共包含总体框架、通信要求、互联协议和应用要求共四部分。总体框架于2021年发布，给出了此系列标准的整体视图。通信要求、互联协议和应用要求均在2023年定稿。规范了异构隐私计算平台间信息交互的通信规则，节点互联、数据互联和算法组件互联时的交互规则以及结合具体场景算法的应用步骤要求。历经三年，跨平台互联互通协议已基本完成。

隐私计算联盟开放协议

随着互联互通的发展，节点互联和资源互联已经形成共识，算法互联最为复杂，中国信通院隐私计算联盟牵头推出了算法互通开放协议，2023年7月相继发布了协议《第 2 部分：SS-LR》和《第 3 部分：PHE-FLR》。《第 1 部分：ECDH-PSI》已在 2022年底发布，后续还会推出专有XGB，专有LR等相关开放协议，助力算法互联。

金融行业团体规范

《金融行业异构隐私计算互联互通平台技术规范》北京金融科技产业联盟于2023年开始制定，旨在制定行业级互联互通统一框架。

这些标准体系里，《隐私计算 跨平台互联互通 开放协议》和《隐私计算 跨平台互联互通》均由信通院牵头编制，一脉相承，其中开放协议是互联协议中算法互联的具体实现，其它标准间的互联互通思路有共性，但仍存在割裂。

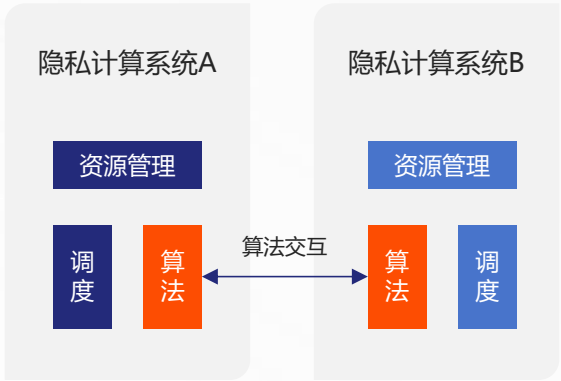
互联互通实践

- **开展丰富的互联互通实践**
  2023年互联互通标准的完善给落地实践提供了统一规范，促成了实践项目成功展开。今年安全多方计算和联邦学习的互联互通实践由节点和资源互联走向了更深层的算法协议互联，不同TEE方案的互联互通研究也出现了新的进展。

一、算法协议互联互通

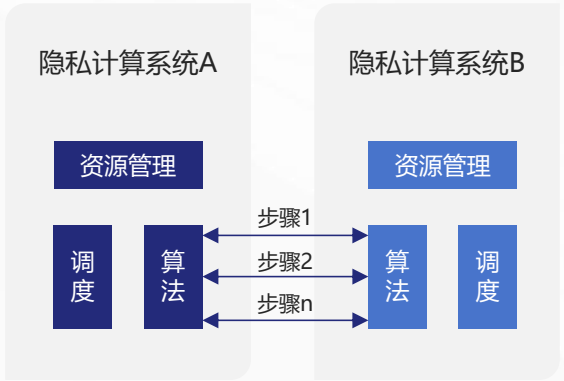
跨开发者算法对齐（黑盒）

2023年隐私计算联盟互联互通实践试点中，中国移动、安恒信息、蚂蚁摩斯分别实现了算法调度层的互连互通，实现了跨平台算法迁移。



跨开发者算法对齐（白盒）

2023年隐私计算联盟互联互通实践试点中，华控清交和联通数字等进行了ECDH-PSI互联互通实践，联通数字、蚂蚁等进行了SS-LR互联互通实践，联通数字、数牍科技等展开了PHE-FLR的互联验证。这些都是开放算法的互连互通，实现了开发者之间的算法对齐。



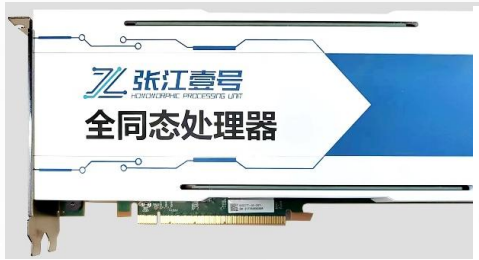
二、TEE的互联互通

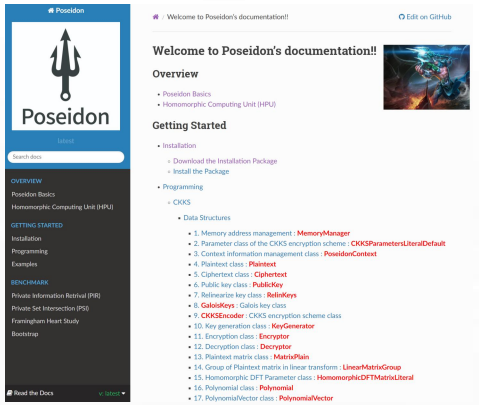
- 工行和蚂蚁牵头推进了北京金融科技产业联盟内TEE的互联互通课题，研究了基于统一远程证明的 TEE 互联互通实践，屏蔽不同TEE方案的差异实现TEE的互联互通。
- 安恒信息推出融合区块链实现去中心化的跨厂商TEE互认证，可信计算平台独立出一个 TEE远程验证代理 模块 ，由代理模块收敛所有远程验证差异化逻辑，其 他 TEE 端借助代理模块完成与对端的远程验证。

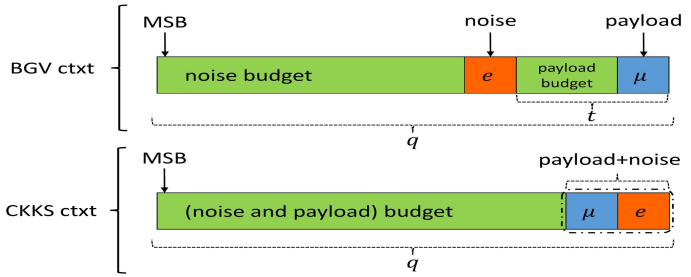
硬件技术

硬件加速技术

在保证安全性的前提下，隐私计算可以通过从硬件、算法、通信、计算方式等多个维度的优化来提升性能。其中，隐私计算硬件扮演非常重要的角色，硬件性能的优劣直接影响数据服务商对外提供隐私计算服务的实时性和用户体验。例如，以全同态加密为代表的隐私计算技术通常引入4至6个数量级的额外计算开销和存储开销。通过设计专用硬件加速算法中的关键步骤可以显著提高计算的效率。中国科学院计算技术研究所在2023年设计出国内首个全同态处理器“张江壹号”，及其配套的全同态专用指令集、算子库Poseidon和硬件加速卡，将全同态加密的硬件性能提升2个数量级。







应用	同态加密方式	明文数据长度	密文数据长度	明文计算时间	密文计算时间
联邦学习模型训练	CKKS	30.5 KB	1.33 GB (5.2万倍)	0.145 秒	390.6 秒 (2694倍)
神经网络推理	CKKS	29.9 MB	546.8 GB (1.9万倍)	212.16 秒	112,026.16 秒 (528倍)
保密数据库查询	BGV	0.71 KB	1.58 GB (40万倍)	0.053 毫秒	7401.49秒 (1.4 亿倍)

软硬件协同技术

- 在硬件提供隐私计算能力的基础上，很多厂商设计相配套的软件系统和硬件协同，通过软件的灵活性将硬件性能发挥到极致。例如，蚂蚁集团的摩斯一体机通过自研的机密计算环境（HyperEnclave、Occlum）和国产CPU芯片提供的安全能力，设计了国产化、自主可控的软硬件体系，为隐私计算提供系统级的解决方案。
- NVIDIA H100 GPU是全球首款具有机密计算功能的GPU，有了基于硬件的强大安全性，用户可以在云上运行应用程序，并保证未经授权的实体无法查看或使用应用程序代码和数据，从而保护了数据的机密性。

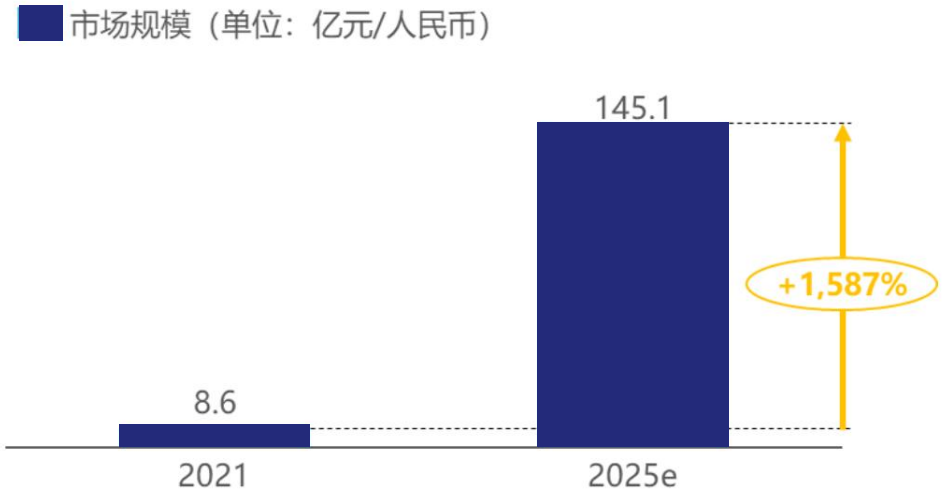
04

第四章：

全球隐私计算应用与市场

应用现状

隐私计算市场空间预测



数据来源：IDC，36氪研究院整理

发展趋势

01 产品与技术成熟度不断提升

隐私计算技术的不断升级，带来了产品的成熟度提升，这也让技术与场景的适配性不断提升，直接扩大了应用市场的规模。

02 密集政策下市场需求的提升

从国家数据局的成立，到全球数据安全相关政策的落地，数据安全作为数据要素安全流通的关键技术，正在被越来越多的机构与企业重视，需求也在不断爆发增长。

03 基于场景实践的解决方案能力提升

伴随着越来越多的场景实践，更多的客户进来探索，隐私计算的综合服务商和垂直服务商们可以对擅长业务场景快速反应，大大提升了市场扩张效率。

国际应用案例

欧盟统计局：处理长期移动网络运营商数据，以了解欧洲各国的经济和社会发展情况。

意大利国家统计研究所和意大利银行：使用保护隐私的记录链接丰富数据分析，以了解该国的经济发展情况。

欧洲统计系统：开发可信计算环境，用于收集和分析欧洲各国的经济和社会数据。

韩国政府采用了安全多方计算技术实现了两个企业的百万级别的数据集的隐私集合求交。

加拿大统计局：使用隐私求交测量数据源的覆盖范围，以了解该国的经济和社会发展情况。

韩国统计局采用了同态加密、安全多方计算以及差分隐私技术将没有信任关系的各个机构与组织的数据进行了整合登记。

加拿大加拿大统计局基于安全多方计算技术开发了一款基于密钥哈希函数的精确隐私数据匹配程序以评估双方的交集大小。

欧盟利用可信的智能调查技术实现数据安全收集

加拿大统计局利用分级同态加密技术对输入数据进行加密并传输到云环境中，在加密数据中训练用于文本分类的神经网络，实现了零售商和服务提供商之间的安全训练。

印度尼西亚旅游部：通过可信执行环境在两个移动网络运营商之间机密共享数据集，以了解该国的旅游业发展情况。

波士顿女性劳动力：通过多方数据隐私计算，以了解该地区的就业情况。

欧盟利用TEE安全处理长期移动运营商的数据

美国使用隐私增强技术推进数据与模型的重复性研究

意大利使用保护隐私的记录链接实现数据分析

美国人口普查局使用差分隐私技术在原始人口数据集上添加噪声，使得数据在被其他机构使用的同时不会披露公民个人信息。

美国教育部使用安全多方计算技术统计分析了全美30个类别本科生的平均贷款与助学金金额。

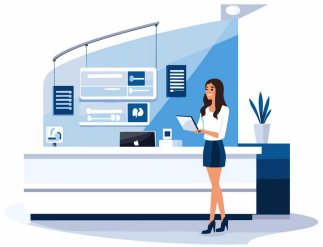
美国众多品牌开始投资搭建数据清洁室，在数据清洁室中，计算是在不暴露彼此数据的情况下进行的，通过这样的处理以防止用户的数据被泄露给广告商。

美国许多的创业公司正在利用零知识证明和安全多方计算技术，这些技术可以让用户在区块链上存储私密数据，同时符合安全规定。

国内主流应用

- 隐私计算已经在金融、通信、政务、医疗、互联网、能源等行业和场景初步商业落地，助力数据价值持续释放。其中在金融、政务、医疗、通信、互联网这几个主要领域持续发展，市场占比超七成，同时在能源、烟草、教育等行业开辟新的应用场景，占比已超过1/10。

政 务



公共数据授权运营+数据发票+公安反诈+准四上企业挖掘+特殊人群福利精准发放+数据招商+群租房监管+区域发展潜力分析+新农村公交路线投放

通过隐私计算技术应用，提升数字城市治理能力，实现政务数据价值“内循环”和“外循环”。结合政务内部数据“内循环”特定场景，实现隐私求交、联合建模、联合统计等应用。在数据安全合规的前提下，政务敏感高价值数据赋能社会，实现政务数据“外循环”，推进政务数据价值的融合计算，实现数字政府高质量转型。

金 融

反欺诈+信贷风控+精准营销+跨境支付+资管+反洗钱+委外催收+供应链金融+保险+普惠金融

金融业是一个数据密集型行业，数据要素的流通为金融数字化转型带来了全新机遇。隐私计算技术在金融数据流通领域中的应用主要包括两个方面。第一个方面是基于密文进行数据处理和安全计算，以保护金融机构的核心资产不被泄露。第二个方面是结合区块链存证、积分激励等机制，设计赏罚分明的积分奖惩机制，实现所有操作上链存证、可追溯，解决数据共享过程中的“不愿共享”问题。

医 疗

医学科研+反医保欺诈+智能问诊+传染病防控+医院数据资产管理+临床数据分析+AI辅助诊疗

医疗领域积累了大量的个人健康数据，其中包括诊断记录、医学影像、病人基因信息等，这些数据在很大程度上推动了医学研究和诊疗的进步，隐私计算作为一种新兴的技术，为医疗行业提供了一种保护隐私和实现数据共享的解决方案，主要应用在医学科研、反医保欺诈、传染病监测防控、医疗数据资产管理等方面。

国内其他应用

- 隐私计算除了应用于政务、金融和医疗三个主流行业外，随着数据流通场景的不断拓展，隐私计算的应用场景也在不断拓展，数交所、互联网、通信、电力、能源、烟草、教育等行业和场景也开始逐步落地，助力数据价值持续释放。

数交所

隐私计算技术可帮助数据交易中心打通包括政务、金融、电信在内的多方数据源，实现与多种数据源的连接和数据的采集，并将来自不同数据源的数据进行集成，实现统一管理。

通　信

通信运营商是海量数据的拥有者，也是数据资源的开发者，隐私计算主要用于产品的营销、结合公安部门数据进行反电诈等。

互联网

互联网行业面临的隐私问题主要是用户数据泄露和滥用，还有数据安全性、黑客攻击等，应用场景主要在于个性化推荐和广告营销。

能　源

能源行业涉及到密集的多方数据采集、分析和应用，如智能电网、智慧能源、新能源汽车等等，隐私计算技术正在逐步落地，实施数据的安全流通和价值挖掘。

教　育

教育机构以及相关研究部门在校园管理、课堂建设、科学研究中涉及到的学生个人隐私数据，正在通过隐私计算技术获得更加可靠的保障。

电　力

电力行业作为数据提供方，将电力数据与政务、金融、交通等行业数据相融合，可以应用于小微信贷风控、税收风险分析、城市数字大脑、精准电桩布网等场景。

烟　草

烟草行业也在积极推进数字化转型工作，数据赋能需要包装数据安全，主要应用场景为精准营销、门店选址、优化物流配送等。

典型应用案例—金融区块链可信共享平台（金易链）

联通数科 Unicom Digital Tech

本案例通过区块链和隐私计算融合技术，在数据安全合规的前提下，实现人民银行、20家商业行、通信运营商等主体间风险信息共享，构建了要素核验、黑灰名单联查、多头/多卡联查、开户码查询等应用场景。搭建了跨机构信息核验和信共享机制，以“数据可用不可见”、“数据不出本地”、“上链存证溯源”为原则，基于国内唯一的“四代+”最高级别组网技术，全球首创“双盲匿踪”模型落地，实现原始数据不出域、计算结果不落盘、处理过程可追溯，消除跨部门数据壁垒。

案例亮点、意义

01

落地应用成效显著

实现原始数据不出域、计算结果不落盘、处理过程可追溯，消除跨部门数据壁垒。目前联盟成员已覆盖20家金融机构，供联盟内查询的数据量已超6000万条，每天查询量近万笔，极大地提升了金融领域风险联防联控的精准度。

02

国内首创“双盲”匿踪算法落地

在多数据源的场景下，联通链双向匿踪查询模块可以通过智能合约对加密分桶进行融合以屏蔽数据来源，保证查询方能获得查询结果，但无法获取结果是谁提供的；被查询方也无法获取查询服务是哪家银行发起的。同时以最小的通信量和计算量实现了多方间的双向匿踪查询，满足金易链百级参与方间的秒级准实时查询需求。

03

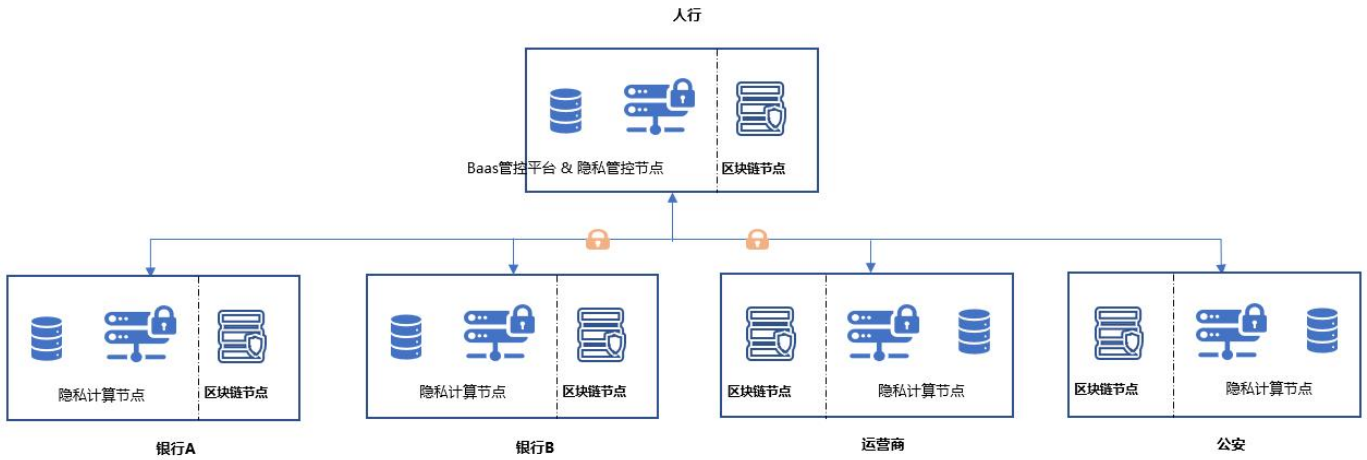
采用国内唯一的“四代+”最高级别的云联网技术

云联网是中国联通推出的新一代MPLS-VPN网络，采用SDN架构技术，是国内唯一的四代+最高级别组网技术，具备超高速度、全智能便利性、全方位兼容性。金易链与云联网的高度适配，打通了众多参与方的复杂网络环境，确保了区块链和隐私计算平台的高速联通。

04

共识算法优化带来平台性能提升

从底层区块链框架开始进行改造，使底链性能在复杂网络环境下达2万TPS以上、实现80%的数据存储和网络传输压降。同时进行了交易生命周期管理优化，使底链在处理亿级交易数据时的性能下降幅度从40%降至7%。



典型应用案例—政务典型案例（联合反诈）

安恒信息 DAS-security 安全中国

公安联合银行反诈场景是指在公安机关与银行之间建立联合机制，共同打击电信网络诈骗活动。公安机关负责收集和分析电信网络诈骗的情报信息，包括犯罪分子的身份信息、作案手法、通信记录等。同时，银行提供相关的金融交易数据和账户信息，协助公安机关追踪犯罪分子的资金流向。基于隐私计算技术，联合建立反诈模型、联合进行风险评估、联合进行资金监测等方式，提高对电信网络诈骗的打击效果。

案例亮点、意义

01

建立公安与银行数据共享机制

在保障数据安全前提下，及时通报诈骗案件信息和犯罪嫌疑人信息，加强信息沟通和协作。

02

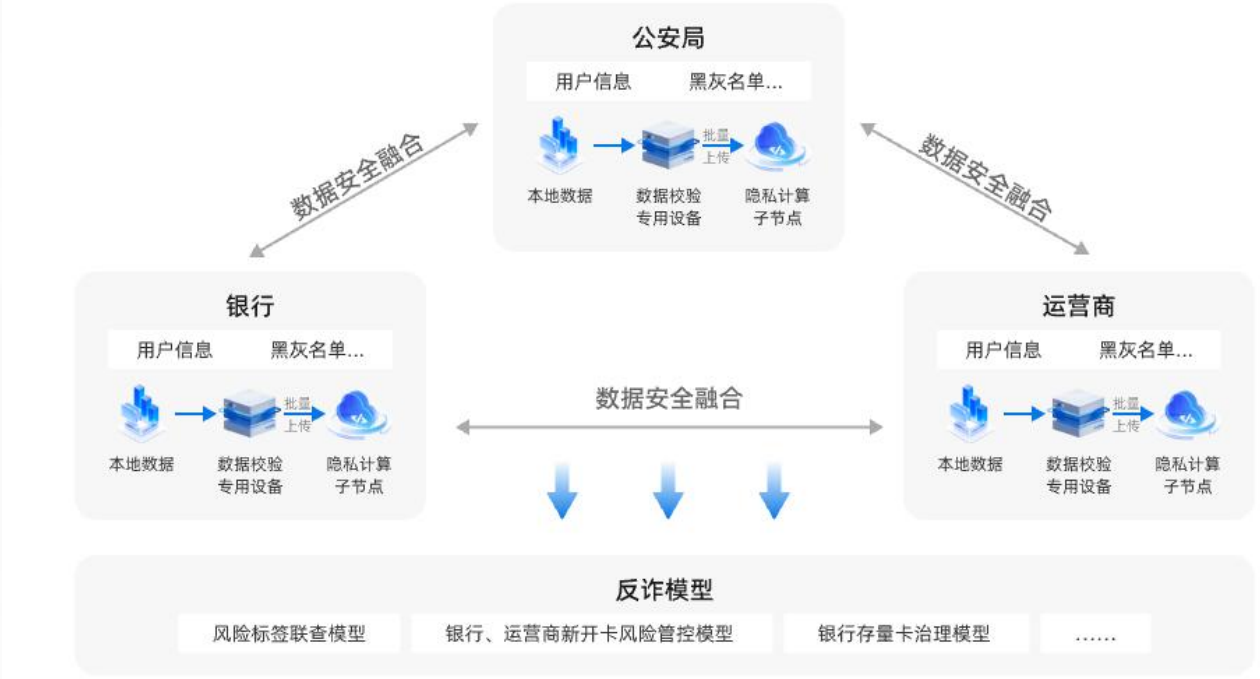
通过多方数据融合，建立客户风险评分卡

通过公安、运营商、银行三家数据标签融合计算，共同制定风险标签联查模型，为每个客户建立一份风险评分卡。

03

通过隐私计算技术手段，精准打击犯罪

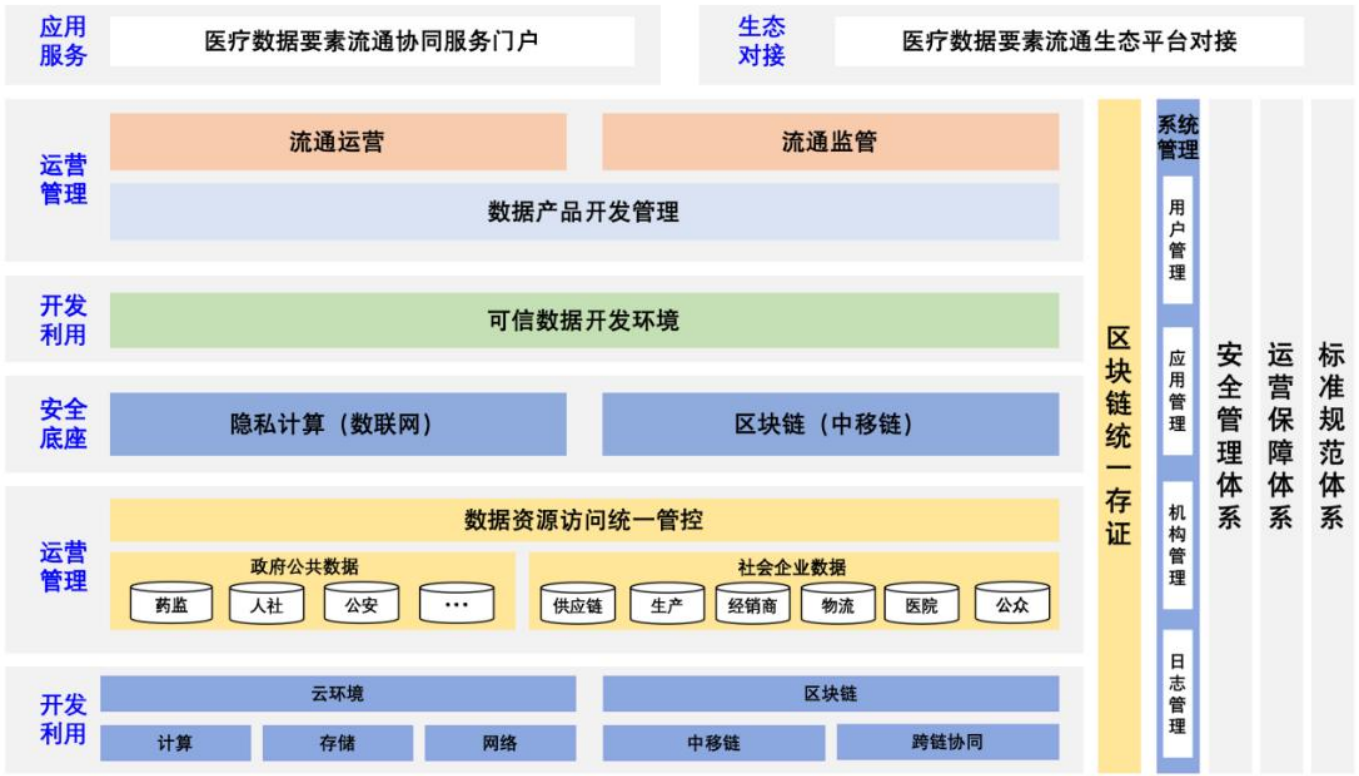
公安利用隐私计算技术，融合多维度、多标签数据，对可疑的金融交易进行监测和分析，精准识别电信诈骗行为，并采取相应的措施进行打击。



典型应用案例—医疗行业数据要素流通平台

中国移动 China Mobile 紫金研究院

本案例基于区块链和隐私计算技术，打造了医疗行业数据要素流通平台。在数据安全合规的前提下，针对医疗产品生产和流通中的各个环节，在充分挖掘数据要素的价值，实现政府可信监管、民众放心用药和企业有效生产。针对政府监管各部委办局、医疗用品生产流通各环节企业和社会公众对医疗用品流通过程中的不同需求，构建医疗物品统一数据集市，在对不同类型数据分级分类管理的前提下，保障医疗用品全生命周期数据机构间、社会化流通。



案例亮点、意义

01 落地应用成效显著

基于平台构建医疗行业统一数据大市场，涉及企业3000余家，数据交易量超亿条。

02 跨平台互联互通统一架构

针对各地数据基础设施建设情况不一的情况，通过建立统一标准，通过标准化协议、规范化接口进行连接，在数据、项目和算法协议三个层面实现异构交互协同，包含统一技术底座和插装式应用服务。

03 数据流通全链路可信监管

结合医疗行业要素流通的全过程，基于区块链底座，构建隐私计算节点管理合约、计算资源管理合约、数据管理合约、项目管理合约、任务管理合约，支撑数据节点认证、数据节点发现、计算资源管理、数据发布、数据授权、任务管控、项目管控和计算组件资源管理。

典型应用案例—AI大模型领域应用-语音识别

LF EDGE

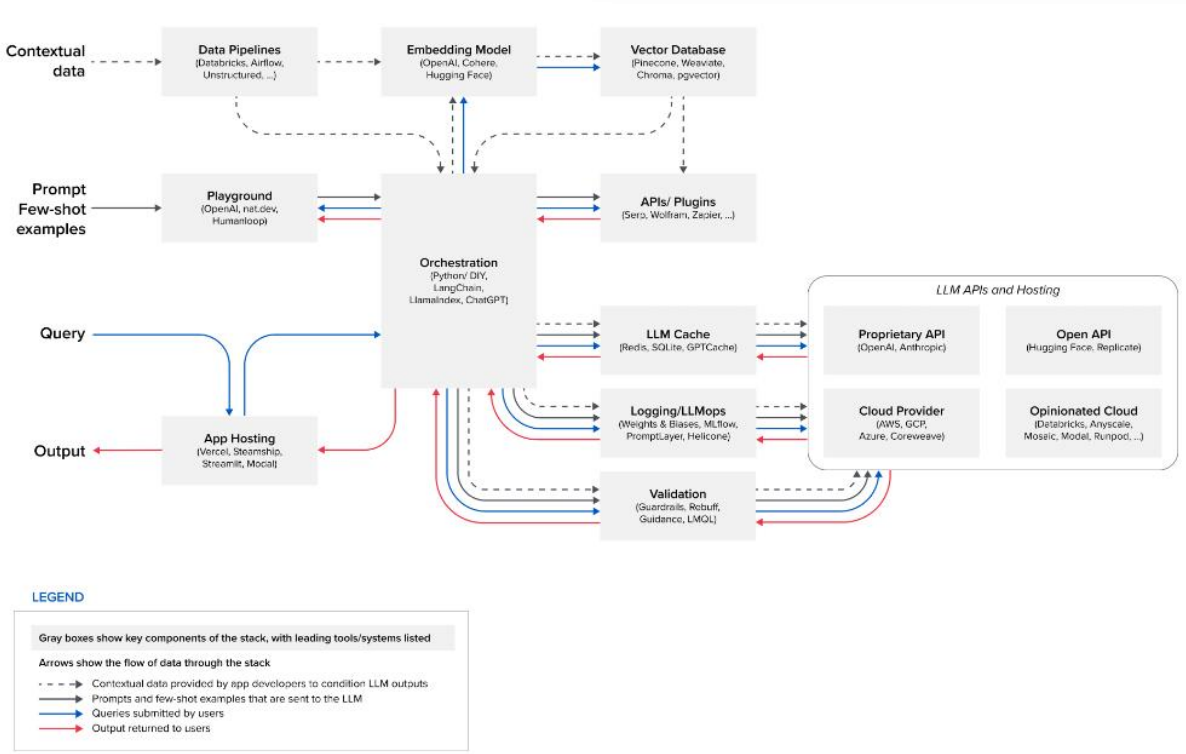
传统的集中式机器学习的框架，可能涉及到敏感个人数据的传输和计算，存在隐私泄露的风险。目前大模型机器学习平台 （比如OpenAI）也有类似的痛点，本案例Linux Foundation Edge AI 的语音大模型通过机密计算架构解决了这个痛点问题，它使用TEE支持whisper model的隐私数据保护，在保护住户隐私的基础上，给大家更好的用户体验。

案例亮点、意义

01 在机器学习中，容易Model 所有权界限职责不清，上传的敏感个人数据在云端计算的时候隐私数据得不到保护，这个系统解决了这个痛点。

02 Model ownership为joint owners， 之前机器学习的数据的所有权非常明确，但是大模型服务中，数据被融合到了模型中，而模型的所有权为模型提供方和多个使用方共同拥有。

03 数据更隐私，为了得到更准确的训练和预测结果，模型使用者会提供更详细， 更隐私的context数据， 这些隐私数据会被上传到云端进行计算。

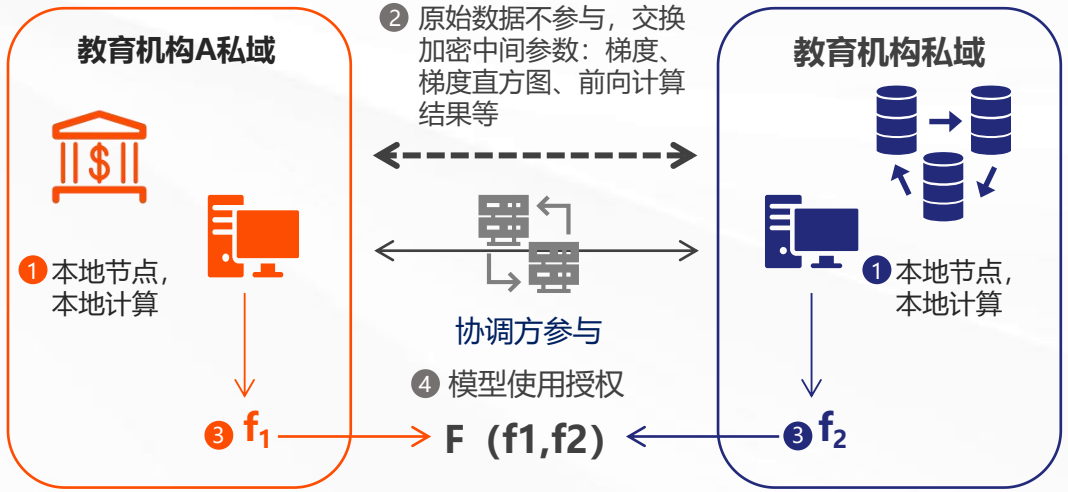


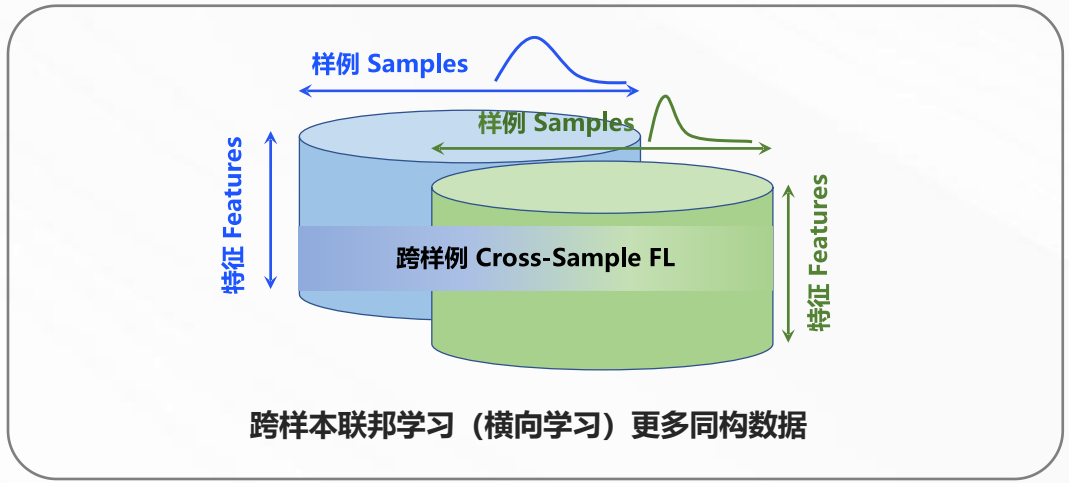
图片来源：https://a16z.com/emerging-architectures-for-llm-applications/

典型应用案例—教育行业跨机构数据安全共享

原语科技 PRIMITIVE HUB　PRIMIHUB

本案例基于横向联邦学习技术，打造了教育行业数据安全共享平台。在保护个人身份信息、学习成绩、行为记录等隐私数据的前提下，针对跨教育机构的数据共享需求，分别在教育机构私域部署隐私计算节点，在保证教育机构原始数据不出本地的前提下，利用联邦学习技术进行信息融合，打造教育研究、学生评估、科研数据整合等联合模型的开发及应用，同时保护个人数据、科研数据等敏感数据免受未经授权的访问和滥用。





案例亮点、意义

01

安全便捷的跨教育机构联合模型建设

通过跨样本联邦学习技术将跨教育机构的模型训练过程迁移到本地设备上，在不共享原始数据的情况下进行模型训练，每个教育机构都可以在本地设备上训练模型，利用自身的数据进行学习，然后通过联邦学习算法，将这些本地模型的更新信息进行聚合，生成一个全局的模型更新。这个全局模型更新再分发给各个教育机构，使得每个机构都能够从整个联邦网络中受益。

02

教育行业隐私计算技术的应用优势

- **数据隐私保护：**
由于原始数据不离开本地设备，跨样本联邦学习可以有效保护教育机构和学生的数据隐私。
- **增加样本多样性：**
跨样本联邦学习可以利用多个教育机构的数据，增加样本的多样性，提高模型的泛化能力。
- **跨机构合作：**
不同教育机构可以共同参与模型的训练，分享模型更新，促进合作与交流。
- **降低通信开销：**
由于只需传输模型更新而非原始数据，跨样本联邦学习可以减少网络通信开销。

典型应用案例—基于隐私计算的全基因组关联分析(GWAS)

锘崴科技 NUOWEI TECH

某三甲医院需要联合多家医院、院校进行有关强直性脊柱炎的全基因组关联分析(GWAS)，全基因组关联分析(GWAS)需要大量样本，单家医院、院校或研究机构的数据量不足以支持，而跨机构基因数据协作和共享又存在隐私安全、数据合规等诸多问题，影响了研究工作的开展。依托锘崴信®隐私计算平台为该医院构建开发了一套跨省级多中心基因数据分析系统，系统融合了多种技术和算法,可实现多家医疗机构数据虚拟聚合，满足全基因组关联分析大数据量需求，达到数据共享和隐私保护的双重目标，帮助研究顺利完成。

方案价值及优势

01 技术框架具有革命性创新价值

该项目开发了一个名为iPRIVATES的技术框架，以往的研究中，都只关注单一技术的设计，而iPRIVATES框架融合了多种技术和算法，可以支持联邦GWAS管道分析的可配置管道，管道设计能够灵活地集成和配置不同的GWAS，方便识别SNPs与许多不同类型的特征之间的关联。

02 效率/精度/安全性等表现优秀

iPRIVATES技术框架在计算精度、算法时间方面都等价于数据物理集中的方式，同时其产生的研究结果，即特征靶点，与集中式计算结果一致。在统计意义上，iPRIVATES 远优于传统计算方式，较之高出一个数量级。

03 可靠性和可推广性获市场验证

基于隐私计算的全基因组关联分析具有一定的可复制性价值和意义，可被迁移到其他疾病的研究中。目前，锘崴科技通过隐私计算技术，已帮助多个病种，连接更多的数据源以提高样本量，帮助医院进行临床辅助诊断以及早期预警工作。

05

第五章：

隐私计算开源选型参考

隐私计算开源选型参考—隐私计算技术开源现状总览

- 作为一个快速发展和注重安全性的技术领域，开源技术可以有效促进隐私计算技术的发展、普及及应用推广，也有利于在行业标准化及互联互通等方面提供更多的参考、方案与范式，从而进一步促进行业的发展与繁荣。
- 国内外隐私计算开源框架与应用工具不断涌现，开源项目涵盖了安全多方计算、联邦学习、可信执行环境、同态加密等各个技术领域。
- 2023年隐私计算开源项目整体趋势：
  - 充分融合：与区块链、图联邦、大模型、大数据等其他技术充分融合，形成更为综合的解决方案；
  - 持续优化：针对应用落地中的实际问题，不断在计算性能、互联互通和部署运维等方面进行优化和完善，以更好地适应现实应用场景；
  - 聚合效应：用户在FATE、隐语等较大型的开源框架上的汇聚趋势更为明显，彰显出开源项目的聚合力。
- 隐私计算开源项目根据技术路径的不同,分为专精单一技术型开源项目和综合技术型开源项目。本报告按照技术路径对开源项目进行分类,并提供多维度分析，给业界同行技术选型提供参考。

综合技术型推荐

综合技术型开源项目同时包含安全多方计算、联邦学习、可信执行环境三大主流技术路线，拥有良好的开源社区生态。这里重点介绍:Syft、SecretFlow和PrimiHub。

项目名称	单位	项目介绍
PySyft	OpenMined	Syft是由OpenMined公司开发的Python开源技术栈，致力于提供安全和私密的数据科学环境。通过采用联邦学习、差分隐私和加密计算等先进技术，Syft实现了类似于numpy的使用方式，并与深度学习框架进行了集成，使得私有数据与横向训练能够有效分离。这意味着数据科学家可以在使用隐私增强技术的同时，保持其当前的工作流程不受影响。Syft允许数据科学家在不获取数据本身的情况下，向数据集提出问题，并在数据所有者设置的隐私限制内获取答案，这一过程被称为远程数据科学。
SecretFlow	蚂蚁集团	SecretFlow是蚂蚁集团推出的统一隐私计算开源框架，专注于保护隐私的数据智能和机器学习。隐语通过实现密文设备和封装了各种密态协议的密态设备的抽象设备层，将高阶算法转化为设备对象流和DAG的设备流层，进而在数据分析和机器学习的算法层使用水平或垂直分区的数据。该框架还在工作流层实现了无缝集成数据处理、模型训练和超参调整等功能，为数据智能和机器学习提供全方位的隐私保护。
PrimiHub	原语科技	PrimiHub是由北京原语科技有限公司开发的综合技术型隐私计算框架。该框架基于安全多方计算、联邦学习、同态加密、可信计算等隐私计算技术构建。PrimiHub具有简单的安装流程，支持Docker一键部署，并提供多种使用方式，包括Web界面、命令行和Python SDK。此框架支持隐匿查询、隐私求交、联合统计、数据资源管理等功能，同时具备灵活配置的自定义扩展语法、语义和安全协议，为用户提供了全面而强大的隐私计算工具。

安全多方计算（MPC）开源项目介绍

- 安全多方计算（Secure Multi-party Computation, SMPC or MPC）指一组互不信任的参与方在需要保护隐私信息以及没有可信第三方的前提下进行协同计算，其涵盖秘密分享、混淆电路、不经意传输等关键技术。
- MPC技术可分为通用MPC技术和专用MPC技术两大类。通用MPC技术指可以支持任何类型计算任务的MPC技术，通常基于混淆电路实现，其通用性好但针对特定问题性能较差。专用MPC技术是针对特定问题构造出的特殊方案，执行效率较高但通用性差，包括四则运算、比较运算、矩阵运算、隐私集合求交、匿踪查询等技术。
- 现有MPC开源项目具有如下特点：大部分框架主要基于秘密共享、同态加密、混淆电路以及相关基本模块的组合；通常使用定制的协议来支持特定数量的参与方（一般为两方或三方），导致可扩展性较差；大多数只能支持诚实大多数/不诚实大多数的半诚实安全模型，以及诚实大多数的恶意安全模型。恶意安全模型只有基于SPDZ协议的安全多方学习框架才可以支持。

编号	项目名称	机构	活跃度	成熟度	功能完整性	性能	易用性
1	MP-SPDZ	CSIRO	★★★★★	★★★★★	★★★★★	★★★	★★★★
2	Private Join and Compute	Google	★★★	★★★★	★★★	★★★	★★★
3	CrypTFlow2	Microsoft	★★★★	★★★	★★★	★★★★	★★★
4	JIFF	Boston University	★★★	★★★	★★	★★★	★★★★★
5	ABY3	Payman Mohassel and Peter Rindal	★★★	★★	★★★★	★★★	★★★
7	OpenCheetah	Alibaba	★★★★	★★★	★★★	★★★★★	★★★
8	FRESCO	Alexandra Institute	★★★	★★★★	★★★★	★★★★	★★★★
10	Sequre	University of Victoria	★★★	★★★★	★★★	★★★★	★★★

活跃度：依据项目的更新频率进行判断；
成熟度：依据项目所发布的版本数量和版本号进行判断；
功能完整性：依据项目所提供功能的完善程度进行判断；
性能：依据项目的执行效率进行判断；
易用性：依据项目使用的便捷程度进行判断；

联邦学习（FL）开源项目介绍

- 联邦学习（Federated Learning, FL）是结合密码学进行安全多方分布式机器学习的技术，是一种可以保证在本地原始数据不出门，只通过传输中间结果进行信息交换完成联合训练机器学习模型的技术。
- 从参与方数据的特征和样例重叠来看，联邦学习落地应用主要分为横向联邦和纵向联邦两大场景。
- 2023年，联邦学习主要针对AI大模型和互联互通展开。

编号	项目名称	机构	活跃度	成熟度	功能完整性	性能	易用性
1	FATE	WeBank	★★★★★	★★★★	★★★★★	★★★★	★★★★
2	FedML	USC	★★★★★	★★★	★★★★	★★★★	★★★★★
3	Flower	ADAP	★★★★★	★★★★	★★★★★	★★★★★	★★★★★
4	TFF	Google	★★★★★	★★	★★★	★★★★★	★★★★★
5	OpenFL	MIT	★★★★★	★★★★★	★★★	★★★	★★★
6	TF-encrypted	TF Encrypted	★★★★	★★★	★★★	★★★	★★★★
7	FederatedScope	Alibaba	★★★★	★★	★★★★	★★★★	★★★★
8	FedLearner	ByteDance	★★★★	★★★★	★★★	★★★	★★★
9	LEAF	CMU	★★★	★★	★★	★★★	★★★★
10	FedLab	SMILELab	★★★★★	★★★★	★★★★	★★★	★★★★
11	Rosetta	MatrixElements	★★★	★★★★	★★★	★★★	★★

活跃度：依据项目的更新频率进行判断；
成熟度：依据项目所发布的版本数量和版本号进行判断；
功能完整性：依据项目所提供功能的完善程度进行判断；
性能：依据项目的执行效率进行判断；
易用性：依据项目使用的便捷程度进行判断；

可信执行环境（TEE）开源项目介绍

- 可信执行环境（Trusted Execution Environment, TEE）通过在硬件设备上构建一个安全区域，保证其内部加载的程序和数据在计算全过程中的机密性、完整性和准确性。与纯软件的密码学隐私保护方案相比，在可信区域内执行的计算逻辑与在明文设备上运行并无差别，所以没有可用性方面的限制，计算表达能力很强，计算效率很高。但在安全性上，TEE技术本身依赖硬件环境，所以必须确保芯片厂商可信，而且与密码学中以数学困难问题保证安全不同，其硬件安全还存在侧信道攻击等其他安全问题。
- 目前，TEE的硬件支持主要基于Intel的SGX以及ARM的TrustZone等技术，主要掌握在国外芯片厂商手里，近两年国内计算芯片厂商海光、飞腾、鲲鹏等也在积极推出自主实现的TrustZone功能。
- 在2023年，针对AI和云原生的需求，提供相应的方案是TEE供应商和开源项目表现出来的新趋势。

编号	项目名称	机构	活跃度	成熟度	功能完整性	性能	易用性
1	Teaclave	百度	★★★	★★★★★	★★★★	★★★	★★★★★
2	OP-TEE	Linaro	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
3	Occlum	蚂蚁金服	★★★	★★★★★	★★★★★	★★★	★★★★★
4	OpenEnclave	Microsoft	★★★	★★★★★	★★★★	★★★	★★★★★
5	Asylo	Google	★★★	★★★★★	★★★	★★★	★★★★★
6	Gramine	OSCAR Lab/Intel	★★★	★★★★★	★★★★	★★★	★★★★★
7	Keystone	UC Berkeley	★★★★★	★★★★	★★★★	★★★★★	★★★★
8	HyperEnclave	蚂蚁金服/阿里云	★★★★★	★★★★★	★★★★	★★★★★	★★★★★
9	Veraison	ARM	★★★★★	★★★	★★★★	★★★★	★★★★★
10	Confidential Cloud Native Primitives	Intel	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★
11	Trusted AI/AIGC Cloud Native Pipeline	Intel	★★★★★	★★★★★	★★★★★	★★★★★	★★★★★

活跃度：依据项目的更新频率进行判断；
成熟度：依据项目所发布的版本数量和版本号进行判断；
功能完整性：依据项目所提供功能的完善程度进行判断；
性能：依据项目的执行效率进行判断；
易用性：依据项目使用的便捷程度进行判断；

06

第六章：

未来趋势

技术趋势

- 技术和产品的未来走向，除了性能提升、安全性提升、国产化替代、软硬件协同、技术融合等赛道的持续突破以外，我们还可以关注以下几点：

数据的质量和真实性挑战。多模态数据复杂性和多样，数据的质量和真实性对隐私计算的结果会产生至关重要的影响，如何保障数据的质量和真实性将成为未来的一大趋势；

01

产品规范化和大规模商用。规范化和商用进程是一个相辅相成的过程，也将是很长一段时间的主流趋势，其中起到助推作用的有三点：
（1）隐私计算相关的标准和指南会加快推出，为落地提供指导参考。
（2）协调数据持有方之间合作推动隐私计算任务将更丰富，破除阻碍，解决数据权属问题。
（3）隐私计算技术应用场景和数据处理规模将越来越大，产品性能也会逐步提升。

02

各开源架构的研发与应用，开源生态加速构建，特别是完全国产化、自主可控的TEE发展势头迅猛，针对国产TEE的攻防实践受到企业重视，安全性得到加强。

03

应用趋势

- **统一数据大市场加快构建，隐私计算有望释放超过十倍的增长空间。**从《关于加快建设全国统一大市场的意见》到《关于加强数字政府建设的指导意见》，再到《数字中国建设整体布局规划》的出炉以及国家数据局的组建，彰显了数字中国建设与数据资源体系在未来国家发展战略中的重要地位，同时意味着安全、高效的统一数据大市场正在加速构建。其中，隐私计算作为促进数据市场化流通与数据安全保障的关键技术，将起到非常关键的推动作用，未来将加快规模化落地应用。但是其中还是有一些挑战需要去突破：

降低技术门槛

各类异构隐私计算平台的互联互通是一个大趋势，算力和经济效益之间的平衡是一个挑战。另一方面计算准确性和提升数据隐私安全性的同时，如何保障性能也是一个突破的方向。特别是对于涉及高敏感、高安全登记数据的业务场景，其计算耗时远高于业务时效性要求。

降低业务使用成本

在传统业务上嵌入隐私计算平台是一件非常耗费成本的事情，但是大部分应用只是局限于小规模、个性化的试点层面，市场的大规模发展仍未到来，这就导致虽然隐私计算能够创造价值，但是规模化依然是一个需要突破的方向。

促进安全合规

数据安全等法规实施后，相应的实施细则和指南出台比较慢，隐私计算落地如何才能合规，这是未来的重中之重。

新应用

- 除了广为讨论的金融、政务、医疗、通信、互联网等领域，个体隐私数据所蕴含价值在新场景中逐步展现，支撑新领域个性化服务需求：

01 智慧城市

城市的智能化运作需要基于居民日常生活的不断反馈，其覆盖范围广泛，如何连接个体在不同生活活动中、不同系统间所产生的生活痕迹，成为沟通智慧城市的基础。通过应用隐私计算，可为智慧城市的建设与运营提供基础底座，打破各系统间的数据交互壁垒、各个体间的数据分享壁垒，实现智能核心的隐私化构建、智能服务的个性化部署。

02 智能养老/复健

有别于医疗机构间的数据交换，从病患个体意愿出发，实现病患状态的持续化跟踪及服务的个性化调配，进而不断定制更智能的辅助设备（如机器人）。（1）个体级别的数据长期感知与存储，（2）相似个体间隐私化知识分享，（3）辅助设备本地化更新部署。

03 自主交通

随着自动驾驶车辆的逐步应用，车辆的网络化控制成为趋势，作为出行过程中个人行为的智能感知设备，对数据的隐私化计算与应用，是实现交通系统自主运行的关键。（1）多模态数据的隐私化计算，（2）车队的隐私化级联控制，（3）数据在不同时空区域的隐私化流转。

新场景

- 跨区域、跨国别数据隐私化交换：突破各国数据保护等相关法律的限制，实现相关业务数据跨区域、跨国别的隐私化交换，进而提升跨区域、跨国别业务的整体能力。（1）数据隐私化流转中间件，（2）相关法律条款制定。

Web3里的去中心化身份

允许实体（通常是用户）利用区块链或其他分布式账本技术以及数字钱包来控制自己的数字身份。去中心化身份的过程涉及到身份匿名、加密存储等，这些都是隐私计算的基础技术架构。有了去中心化身份，用户才能在诸如元宇宙、Web3体系中构建信任机制。

数字人民币货币桥

多边货币桥将不同国家或地区发行的中央银行数字货币连接起来，允许数字货币之间进行跨境交换和互操作，为数字货币的互联互通提供了关键基础。相较传统模式下的代理行转账，数字人民币货币桥课实现“点对点”支付的实时结算，大幅提升了支付效率，助力人民币的国际化。

元宇宙的未来可能

具备持久性，提供增强的沉浸式体验。元宇宙的核心在于数字映射，如何将现实场景数字化、虚拟化，这涉及到隐私保护交易、隐私保护应用、隐私保护建模、隐私计算网络、隐私边缘计算等许多隐私计算相关技术体系。

鸣谢单位

- 北京航空航天大学
- 北京交通大学
- 北京原语科技有限公司
- 北京江南天安科技有限公司
- 广州大学
- 华为技术有限公司
- 杭州安恒信息技术股份有限公司
- 杭州锘崴信息科技有限公司
- Linux Foundation Edge
- 联通数字科技有限公司
- 山东大学
- 上海处理器技术创新中心
- 中关村实验室
- 中山大学
- 中国科学院计算技术研究所
- 中国网络空间研究院
- 中国移动紫金(江苏)创新研究院有限公司

（排名不分先后，以拼音首字母排序）

致　谢

在此，感谢所有支持和参与编写《2023全球隐私计算报告》的政企单位、研究机构和行业专家，感谢所有关注隐私计算行业发展、贡献开源的各界人士。

欢迎与我们联系探讨报告内容

主编：熊婷 杭州数据协同创新未来实验中心副主任

设计：赵宁、冯帅