2022中国隐私计算产业研究报告

目录

CONTENTS

报告摘要

发展环境

在数据上升为与土地、劳动力、资本、技术并列的生产要素的大背景下，多项政策提出要加快培育数据要素市场。隐私计算可帮助推进政府数据开放共享，研究建立公共数据开放和数据资源有效流动。

产业趋势

隐私计算场景应用实践的加深将会在不同程度上同频带动算力加速需求的增加，算力加速将成为重要竞争力；隐私计算未来生态主要由数据源、数据使用方和服务商参与，开源产品已成为生态中的主流。

应用现状

目前市场上隐私计算应用最多的领域主要为金融、政务和医疗，其中应用最成熟的是银行业、保险业，隐私计算在资管行业发展相对较慢，政府与医疗场景具有极大发展潜力。

机遇挑战

隐私计算产品目前会造成用户对性能与安全性二选一的抉择，并且隐私计算产品在算法协议、开发应用方面安全性仍有不足，一体机成为目前落地最为广泛的软硬一体解决方案。

名词解释

- RSA：一般指RSA算法，一种使用不同的加密密钥与解密密钥，“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制
- 同态加密：基于数学难题的计算复杂性理论的密码学技术；对经过同态加密的数据进行处理得到一个输出，将这一输出进行解密，其结果与用同一方法处理未加密的原始数据得到的输出结果是一样的
- TEE：Trusted Execution Environment，可信执行环境，通过软硬件方法在中央处理器中构建一个安全区域，保证其内部加载的程序和数据在机密性和完整性上得到保护
- 联邦学习：一种分布式机器学习技术，其核心思想是通过在多个拥有本地数据的数据源之间进行分布式模型训练，在不需要交换本地个体或样本数据的前提下，仅通过交换模型参数或中间结果的方式，构建基于虚拟融合数据下的全局模型，从而实现数据隐私保护和数据共享计算的平衡
- GPU ：Graphics Processing Unit，图形处理器，是一种专门在个人电脑、工作站、游戏机和一些移动设备（如平板电脑、智能手机等）上做图像和图形相关运算工作的微处理器
- FPGA：Field Programmable Gate Array，现场可编程门阵列，作为专用集成电路领域中的一种半定制电路而出现的，既解决了定制电路的不足，又克服了原有可编程器件门电路数有限的缺点

一、隐私计算产业发展现状分析

概念界定：保证提供方不泄露原始数据，对数据分析计算的一系列信息技术

◆2016年4月，通信学报上刊登的《隐私计算研究范畴及发展趋势》将隐私计算定义为是面向**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。

◆2019年，《隐私计算 ——概念、计算框架及其未来发展趋势》一文将隐私计算定义为是面向**隐私信息**全生命周期保护的计算理论和方法，具体 是指在处理**视频、音频、图像、图形、文字、数值、泛在网络行为信息流**等信息时，对所涉及的隐私信息进行描述、度量、评价和融合等操作， 形成一套符号化、公式化且具有量化评价标准的隐私计算**理论、算法及应用技术**，支持多系统融合的隐私信息保护。

◆2021年，中国信息通信研究院云计算与大数据研究所在《隐私计算法律与合规研究白皮书》中将隐私计算定义为在**保证数据提供方不泄露原始 数据的前提下，对数据进行分析计算的一系列信息技术**，实现数据在流通与融合过程中的“可用不可见”。

亿欧智库：隐私计算的特征

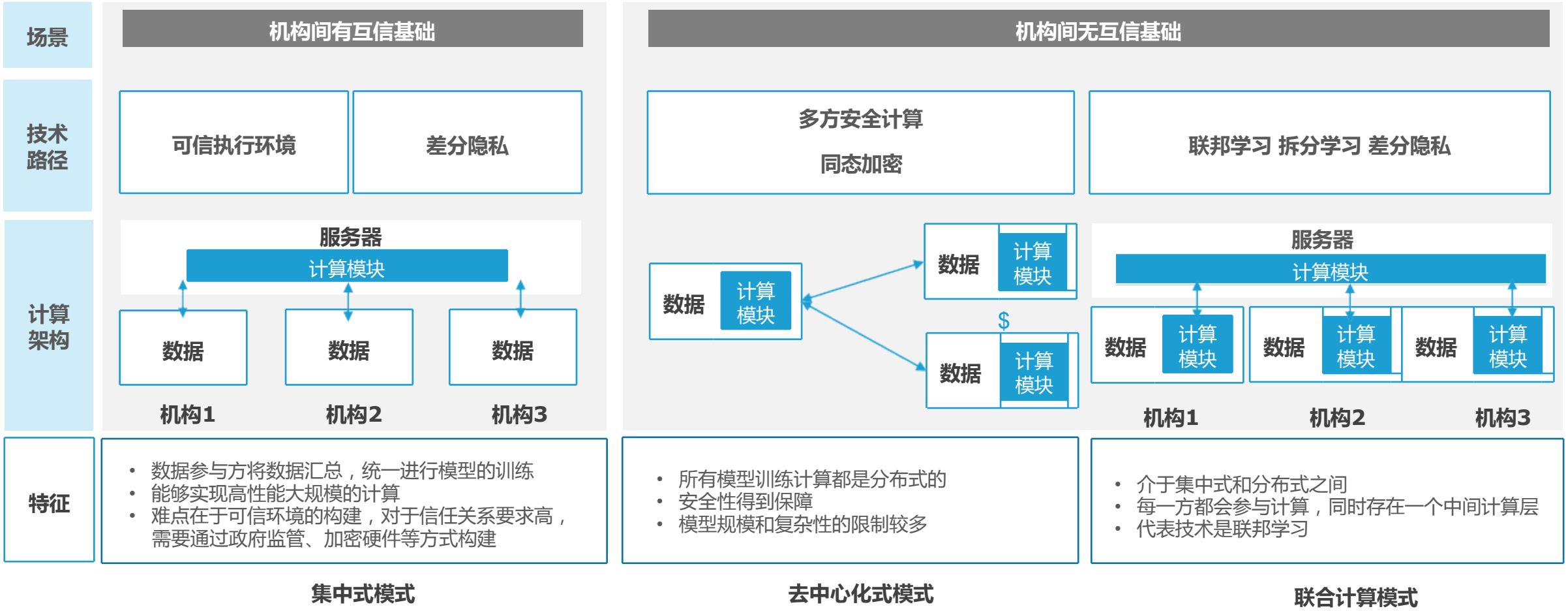
- 一般的隐私计算应用中，通常至少有两个参与方，部分参与方可承担两个或两个以上的角色。
- 数据计算方需保证输入隐私：参与方不能**在非授权状态下获取或者解析出原始数据及中间计算结果。**
- 数据计算方需保证输出隐私：参与方不能**从输出结果中反推出敏感信息。**

数据来源：公开资料，亿欧智库整理

隐私计算特征

◆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不透明状态下的计算，以达到各参与方隐私保护的目的。隐私计算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。它能够保证满足数据隐私安全的基础上，实现数据“价值”的流通与共享，真正做到“数据可用不可见”。

基于隐私保护计算的“跨机构”数据协同模式



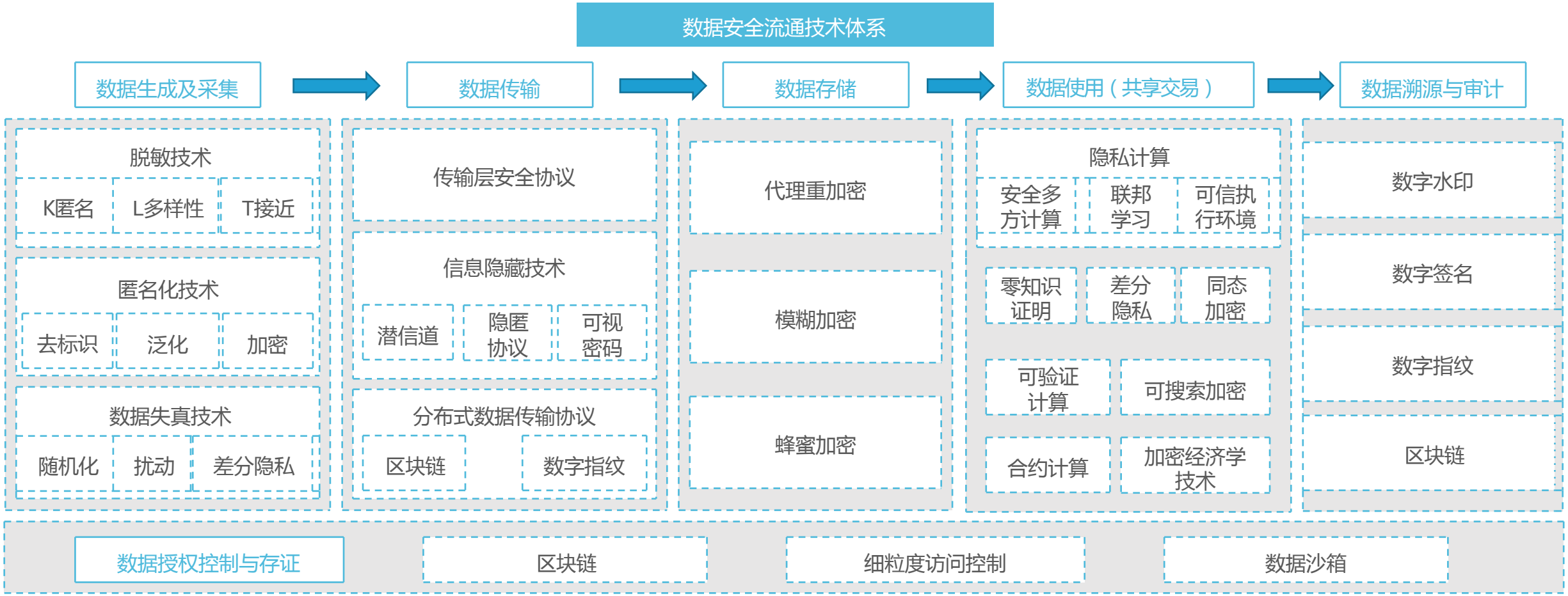
数据来源：蚂蚁隐语、亿欧智库整理

隐私计算的重要意义

◆为了实现数据“可用不可见、可用不可存、可控可计量”的安全流通，数据安全流通技术体系由**数据生成及采集、数据传输、数据存储、数据使用（共享交易）、数据溯源与审计五个环节组成。**

◆其中，隐私计算是指数据使用环节中所使用的隐私保护的数据计算技术。

亿欧智库：隐私计算在数据安全流通中的定位和环节



数据来源： Datafun、中国信通院、亿欧智库整理

隐私计算产业发展历程：从密码学到人工智能

◆ 目前，国内的隐私计算业界将隐私计算相关技术概括为三个大类，分别为**以安全多方计算为代表的密码学路径、以可信任执行环境为代表的硬件路径和以联邦学习为代表的人工智能路径。**

密码学路径——安全多方计算\同态加密

1978年 随着非对称式加密算法RSA的出现，同态加密的概念被首次提出。

-Rivest R, et al.On Data Banks and Privacy Homomorphisms. 1978

1982年 姚期智教授提出了百万富翁问题，引入了安全两方计算。1987年由GMW拓展到安全多方计算。

-Yao AC.Protocols for secure computations. 1982

2017年，国际同态加密委员会成立，标志着同台加密在全球进入高速发展阶段。

-Application of Homomorphic Encryption Standard.2017

2019年，由阿里巴巴牵头的MPC联盟成立，并开始推进相关IEEE国际标准，标志着MPC进入商业发展阶段。

-MPC Alliance

硬件路径——可信执行环境

2009年 OMTP提出了TEE标准。2015年Intel发布首款支持TEE方案的CPU，Intel SGX.

-OMTP. Advanced Trusted Environment: OMTP TR1. 2009

2016年 王爽教授团队完成了基于TEE和安全联邦学习的全球首例支持跨多个国家的罕见病跨国医疗数据隐私保护下的互联互通，并获得Intel杰出贡献奖。

-Bioinformatics，vol.33,no.6, p871

2018年 百度发布Mesa TEE解决方案。2020年阿里巴巴发布Occlum TEE系统，可信计算环境进入高速商用发展阶段。

-Mesa开源：隐私保护的高性能通用安全计算终成现实-百度安全社区，2021

人工智能路径——联邦学习

2012年 王爽教授团队发表了全球首篇医学在线安全联邦学习文件，提出了“数据可用不可见”的问题和解决隐私计算的基础性框架和联邦学习的工程落地方案

-“EXPLORER”，Blomed，Inform，2013

2016年 Google提出了联邦学习在移动互联网上应用的概念，隐私计算技术被认可并进入快速发展阶段。

-J Konecyet al，“FL：Strategies for Improving Communication Efficient” ArXiv,2016

2018年 杨强教授团队携手腾讯/微众银行，用联邦学习技术发布了开源项目FATE。

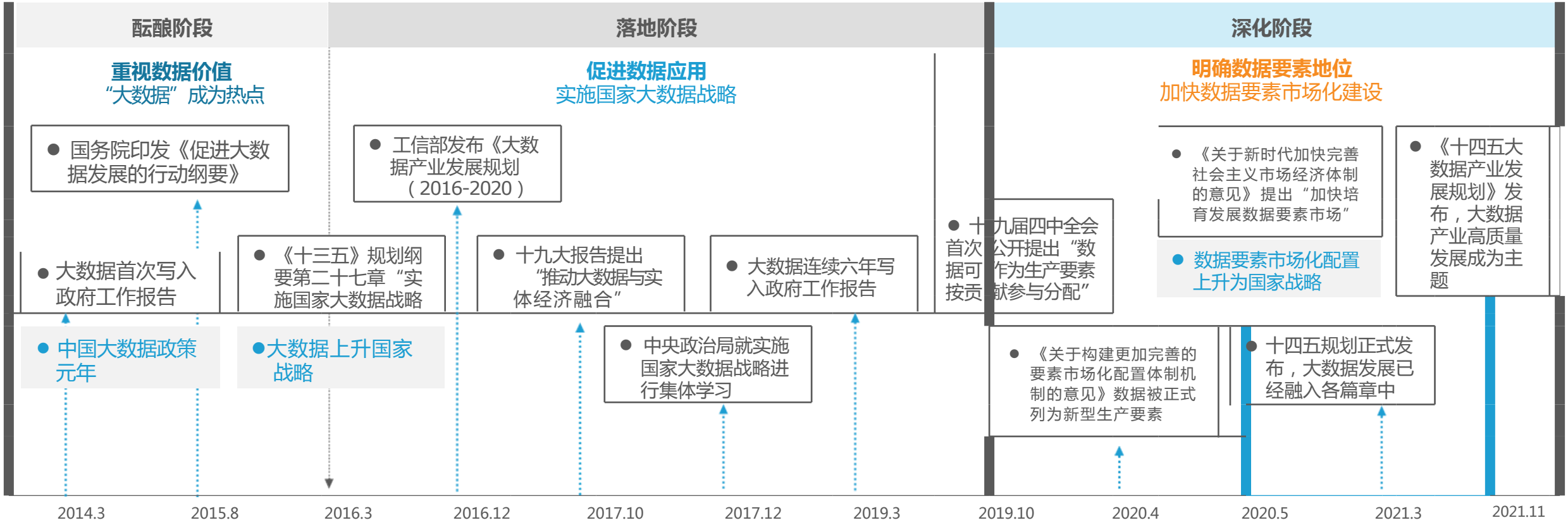
数据来源：公开资料，亿欧智库整理

隐私计算政策历程：充分发挥数据要素价值，安全可控驱动隐私计算发展

◆作为数字经济时代的新型生产要素，数据的价值日益被充分认可。2020年，国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，将数据上升为与土地、劳动力、资本、技术并列的生产要素，提出要加快培育数据要素市场。**推进政府数据开放共享，研究建立公共数据开放和数据资源有效流动的制度规范。**

◆国家《“十四五”数字经济发展规划》也明确提出要充分发挥数据要素作用、强化高质量数据要素供给，加快数据要素市场化流通，创新数据要素开发利用机制；加快构建数据要素市场规则，培育市场主体、完善治理体系，到2025年初步建立数据要素市场体系。**这标志着我国数字经济发展转向以“数据要素市场”为核心的普惠共享、深化应用的新阶段。**

亿欧智库：我国数据战略布局历程



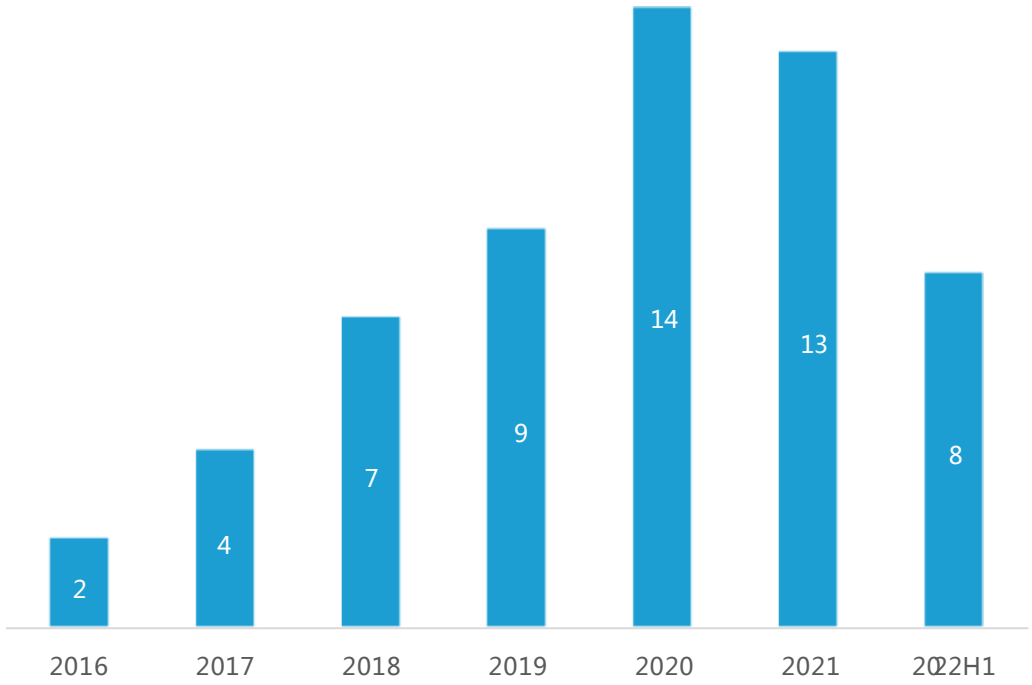
数据来源：亿欧智库整理

资本市场：隐私计算投融资热度逐年上升

◆风口之上，“追风者”蜂拥而至。互联网巨头、网络安全、大数据公司、初创型科技企业及行业数据高度聚合型企业纷纷入局。根据国家工业信息安全发展研究中心发布的《中国隐私计算产业发展报告（2020-2021）》显示，**2021年隐私计算产品市场规模约为10亿元，基于隐私计算的数据交易应用模式市场或将达到千亿级。**

◆从2016年至2022年上半年，隐私计算初创公司累计获得57笔股权融资，公开披露的融资总额达到56.1亿元（12笔未透露金额），笔均融资多在千万级规模。其中2020年与2021年热度较高，就2022年上半年表现来看，热度仍在持续提升。

亿欧智库：2016-2022上半年中国隐私计算行业投融资事件数



亿欧智库：2021全年中国隐私计算行业主要投融资事件

单位：人民币（元）

企业名称	投资轮次	融资金额	企业名称	投资轮次	融资金额
数蓬科技	B&B+	约5.5亿	富数科技	C	数亿
宇链科技	A+	数千万	翼方健数	B+	超3亿
洞见科技	Pre A	数千万	冲量在线	Pre A	数千万
趣链科技	C	数亿	锘威科技	B	数亿
星云Clustar	A+	数千万	同态科技	Pre A	数千万
云象区块链	B	数亿	华控清交	B	7亿
数泰科技	A	数千万			

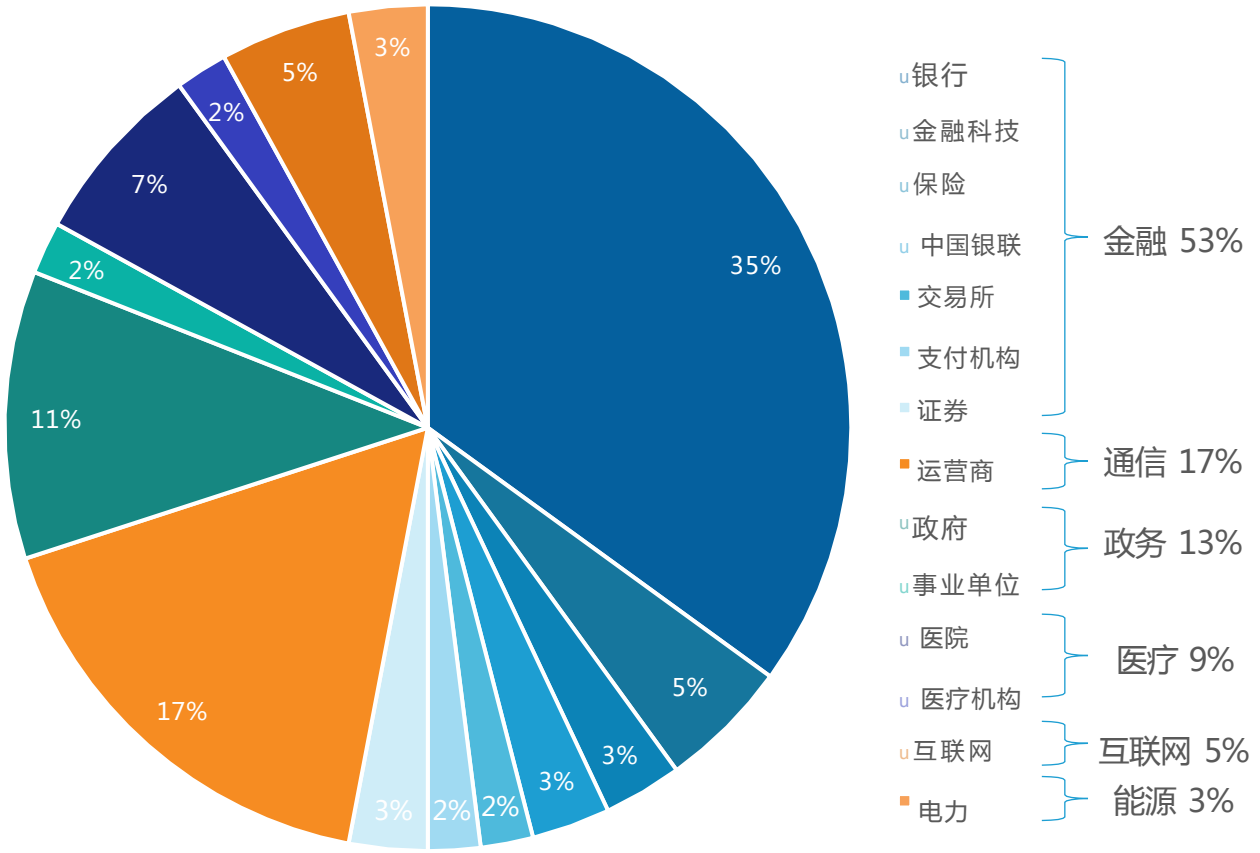
数据来源：公开资料，亿欧数据，亿欧智库整理

隐私计算产业应用现状与市场规模

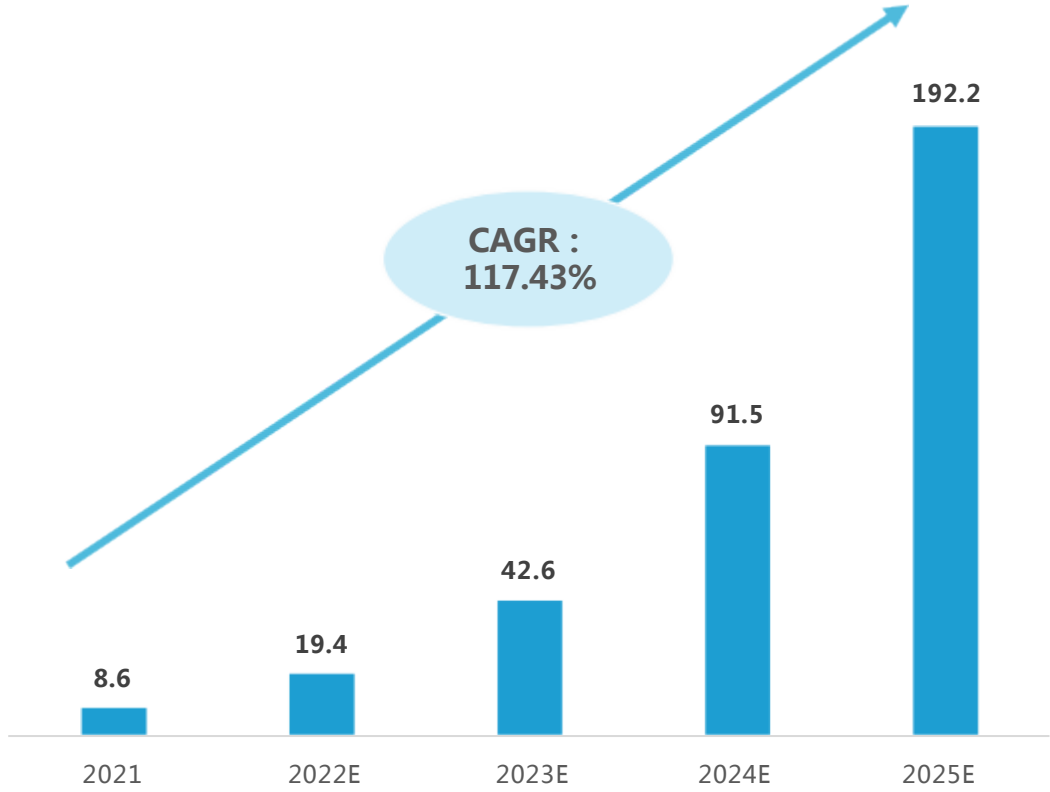
◆隐私计算目前主要应用行业为金融、通信、政务和医疗，未来的市场增量主要来自于传统数据流通方式的转变，其中包括存量数据流通方案的重构，以及传统流通方案下无法流通的数据在隐私计算流通方案中实现合规共享。

◆隐私安全计算的价值被看到后，包括阿里巴巴、微众银行、蚂蚁集团、平安科技等多家公司已积极布局隐私安全计算，并推动技术应用。根据中国信通院调研数据显示，2021年约有44%的隐私安全计算产品进入实施阶段，占比进一步提升；处于研发阶段的隐私安全计算产品占比相对下降，占比为19%。

2019-2022H1年隐私计算招标行业比例

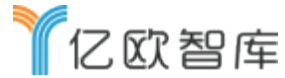


2021-2025年隐私计算市场规模推算（亿元）



数据来源：中国信通院，亿欧智库整理

隐私计算产业图谱



上游可信硬件

CLUSTAR 星云
HYGON 中科海光
Phytium 飞腾
AMD
HISILICON
intel
arm CHINA
NVIDIA

中游技术提供方

隐私计算垂直企业

Base Bitai
CLUSTAR 星云
华控清交 HUA KONG TSINGJIAO
洞见科技 INSIGHTONE
富数 FUDATA.CN
数牍 sudo
融数联智

综合科技类企业

Tencent 腾讯
HUAWEI
阿里巴巴
蚂蚁集团 ANT GROUP
China unicom 中国联通
美团
Baidu 百度
京东云

大数据企业

TRANSWARP
医渡云
隔镜科技 Trust Mirror
慧联科技
同盾科技
DataExa
京信大数据
八分量

金融科技企业

百融云创
WeBank 微众银行
翼支付
度小满金融
招商银行
pd

硬件产品服务

蚂蚁集团 ANT GROUP
富数 FUDATA.CN
Baidu 百度
洞见科技 INSIGHTONE
冲量在线
CLUSTAR 星云

AI服务企业

科大讯飞 iFLYTEK
RealAI
oascamia
4Paradigm 第四范式
水母智能 SMALL DESIGN

信息安全企业

360 数科
CETC 中国网安
奇安信
DBAPPSecurity 安恒信息
NSFOCUS

云服务企业

华为云
UCLOUD 优刻得
阿里云
天翼云 e Cloud
Westone 卫士通
腾讯云
奇点云
GrowingIO
百融云创

区块链企业

Ant BlockChain
零数科技
AIBI

开源产品

天冕
同盾科技
原语科技 PRIMITIVE HUB
Baidu 百度
矩阵元
字节跳动
BaseBit.ai

下游行业应用方

金融

通信

China unicom 中国联通
中移软件 CMSoft
中国移动 China Mobile
中国电信

互联网

Baidu 百度
Tencent 腾讯
蚂蚁集团 ANT GROUP

政务

山东省大数据局
系山东数据交易有限公司

医疗

华大生命科学研究院 BGI·Research
浙江大学滨江研究院

数据来源：亿欧智库整理

二、隐私计算产业发展趋势分析

产业技术趋势分析——隐私计算厂商关注算力加速

◆**算力加速将成为重要竞争力**：隐私计算场景应用实践的加深将会在不同程度上同频带动算力加速需求的增加，在隐私计算跨平台互联互通推动下的场景应用实践的加深，算力加速需求都迎来了同频增长，算力加速将成为重要竞争力。

◆性能由算法协议、计算流程、系统架构、数据规模、软硬件环境、网络带宽等多种因素共同决定：

- 在算法优化层面，算法加速，尽可能降低子模块耦合度，对算法流程重新进行深度编排
- 在硬件加速层面，通过新的密码学技术和算法协议，结合硬件加速技术（如GPU、 FPGA、ASIC加速）和专有算法实现硬件来加速计算量较大的环节和步骤，也能够有效提高性能

亿欧智库：隐私计算各技术路径多维度对比

技术路径	计算过程保护	计算结果保护	计算性能	计算精度	硬件依赖	理论支持场景	已商用场景	计算模式
安全多方计算	最好	无	较差	最好	无	任意计算	国际：拍卖、薪资统计、密钥管理 中国：密钥管理、联合建模	分布式
联邦学习	较好	无	较好	最好	无	机器学习建模	国际：横向联邦学习（Google GBoard） 中国：纵向联邦学习（金融风控）	分布式
可信执行环境	较好	无	最好	最好	有	任意计算	国际：密钥管理 中国：联合建模、区块链	中心化
差分隐私	较差	有	较好	较好	无	任意计算	Google GBoard	中心化
同态加密	最好	无	较差	较好	无	任意计算	无	中心化
零知识证明	较差	无	较差	较差	无	任意计算	区块链	分布式

数据来源： DAMA，专家访谈、亿欧智库整理

产业生态趋势分析——隐私计算拥抱开源

◆开源社区的知识共享和多方协同有利于加快技术升级迭代和商业化项目落地的效率。对比传统的大数据技术工具，开源已成为生态中的绝对主流。作为保障数据合作与安全的重要基础，隐私计算有望进一步拥抱开源。

开源生态成为潮流

在隐私计算领域，开源能够快速推动行业整体发展，上中下游都将软件开源，使各方可针对不同应用场景，运用技术手段，根据各自需求进行调整，极大提高隐私计算各环节的技术发展效率，使整个生态链更加完善。

多方生态融合发展共同推进

随着开源环境下的隐私计算技术不断发展，隐私计算发展和应用落地需要包括法规体系、技术体系、应用体系等多方生态的融合。

亿欧智库：不同技术路径开源项目举例

项目名	机构	技术路径
PySyft	Open Mined	多方安全计算、联邦学习
TF-Encrypted	Dropout Labs、Openmined、阿里巴巴	多方安全计算
Asylo	谷歌	可信执行环境
MesaTEE	百度	可信执行环境
FATE	微众银行	联邦学习
TF-Federated	谷歌	联邦学习
Private Join & Compute	谷歌	多方安全计算
Paddle FL	百度	联邦学习
CrypTen	Facebook	多方安全计算
Fedlearner	字节跳动	联邦学习
Rosetta	矩阵元	多方安全计算
KubeTEE	蚂蚁集团	可信执行环境

数据来源： DAMA，专家访谈，亿欧智库整理

法规

法规体系需加速完善，作 数据安全治理和建设的顶层指导，有助于 更 好 地理解安全场景与需求 进 而有利于将隐私计算 技术实际落地与应用

应用体系需进一步加强，目前主要在金融、运营商、医疗、政务数据等行业，存在成功的隐私计算应用案例，但多数领域仍处于试点应

界加强 应 隐 要

技术

开源协同加速隐私计算技术迭代，技术开源，已经全面渗透到信息技术的各个领域，未来发展趋势必将是开源平台与自研平台并存，产学研用合作形成既开放又独特的多元生态。

产业应用趋势分析——隐私计算产业生态由三方参与

◆隐私计算未来产业生态将由数据使用方、数据源与隐私计算服务机构三方参与。其中数据使用方与数据源两方存在重叠，隐私计算服务机构作为中间人或手段提供者 ，促进行业内部或跨行业的数据流通运转。

亿欧智库：隐私计算未来产业生态

◆隐私计算服务商目前有三种商业模式：

1 **硬件销售**

目前隐私计算领域硬件产品主要有两种FPGA加速卡与隐私计算一体机，作用均为提升隐私计算性能，更加符合实际应用场景需求
典型产品：星云Clustar隐私计算：软硬件一体机、蚂蚁摩斯隐私计算一体机等

2 **软件销售**

多数隐私计算业务的公司均提供隐私计算系统软件销售
典型产品：蚂蚁摩斯多方安全计算平台、华控清交PrivPy多方安全计算平台、同盾科技智邦平台iBond、瑞莱智慧隐私保护机器学习平台RealSecure、天冕科技的天冕联邦学习平台WeFe、洞见科技INSIGHTONE洞见数智联邦平台等

3 **平台分润**

隐私计算公司软件销售积累了一定数量的客户之后，客户通过软件平台调用数据，获得收益之后，隐私计算公司抽取平台提成。主要有数据源侧分润、数据应用场景分润以及类数据代理模式

数据来源：专家访谈，亿欧智库整理