

2022中国隐私计算产业研究报告

亿欧智库 <https://www.iyiou.com/research>

Copyright reserved to EqualOcean Intelligence, October 2022

目录

CONTENTS

1. 隐私计算产业发展现状分析
2. 隐私计算产业发展趋势分析
3. 隐私计算典型应用场景分析
4. 隐私计算产业发展机遇与挑战

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。

- ◆ 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”。

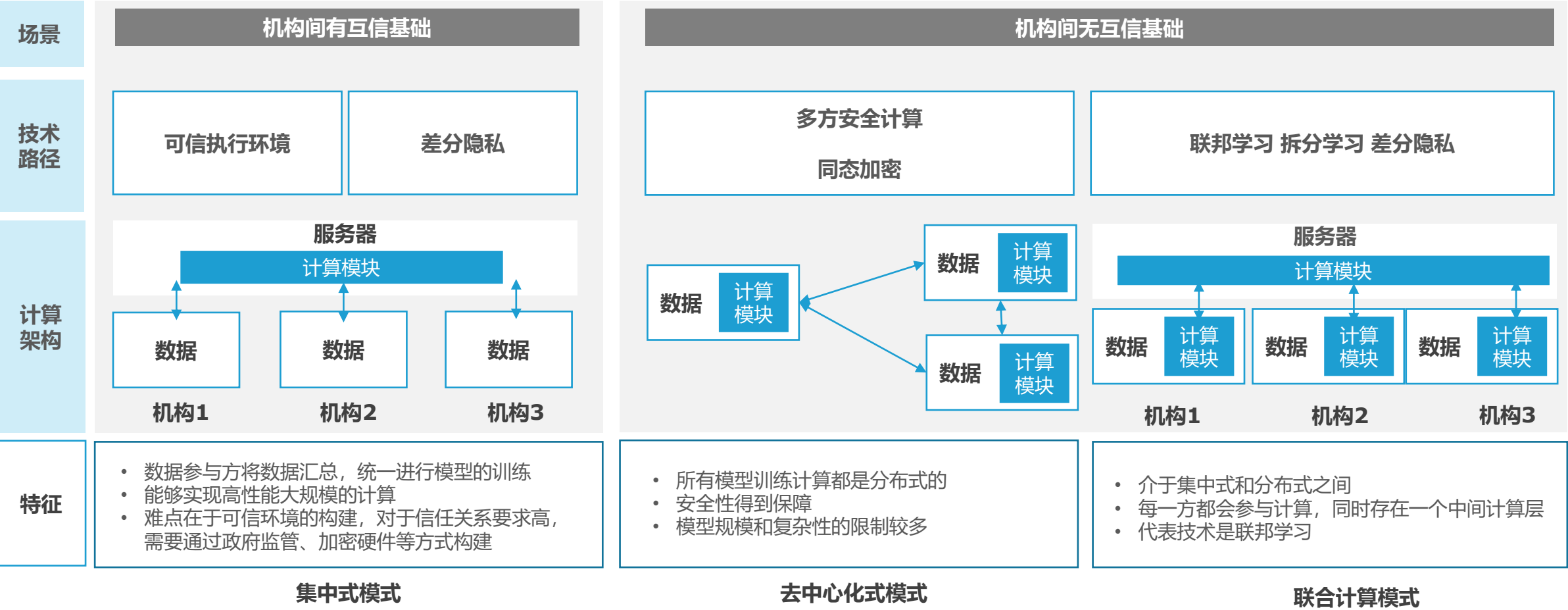
亿欧智库：隐私计算的特征



- 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**。

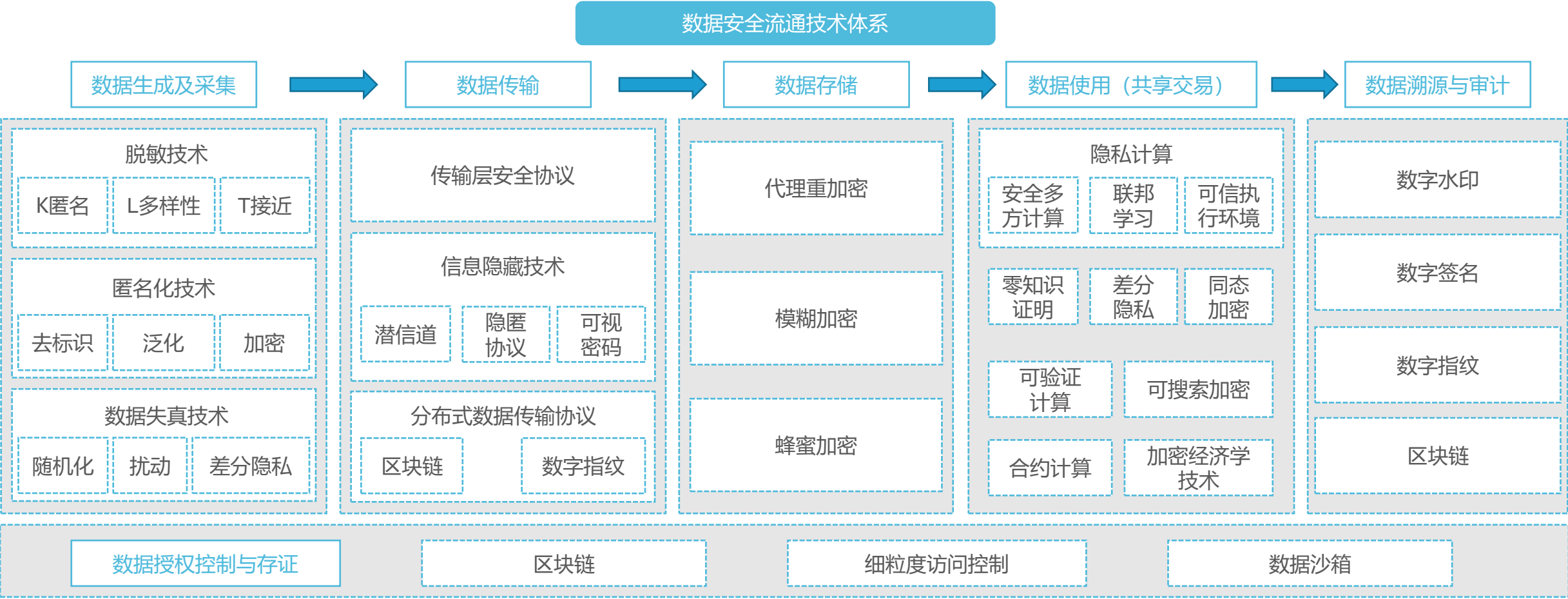
◆ 面对数据计算的参与方或其他意图窃取信息的攻击者，隐私保护计算技术能够实现数据处于加密状态或不透明状态下的计算，以达到各参与方隐私保护的目。隐私计算是一套包含人工智能、密码学、数据科学等众多领域交叉融合的跨学科技术体系。它能够保证满足数据隐私安全的基础上，实现数据“价值”的流通与共享，真正做到“数据可用不可见”。

基于隐私保护计算的“跨机构”数据协同模式



- ◆ 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



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，标志着同态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

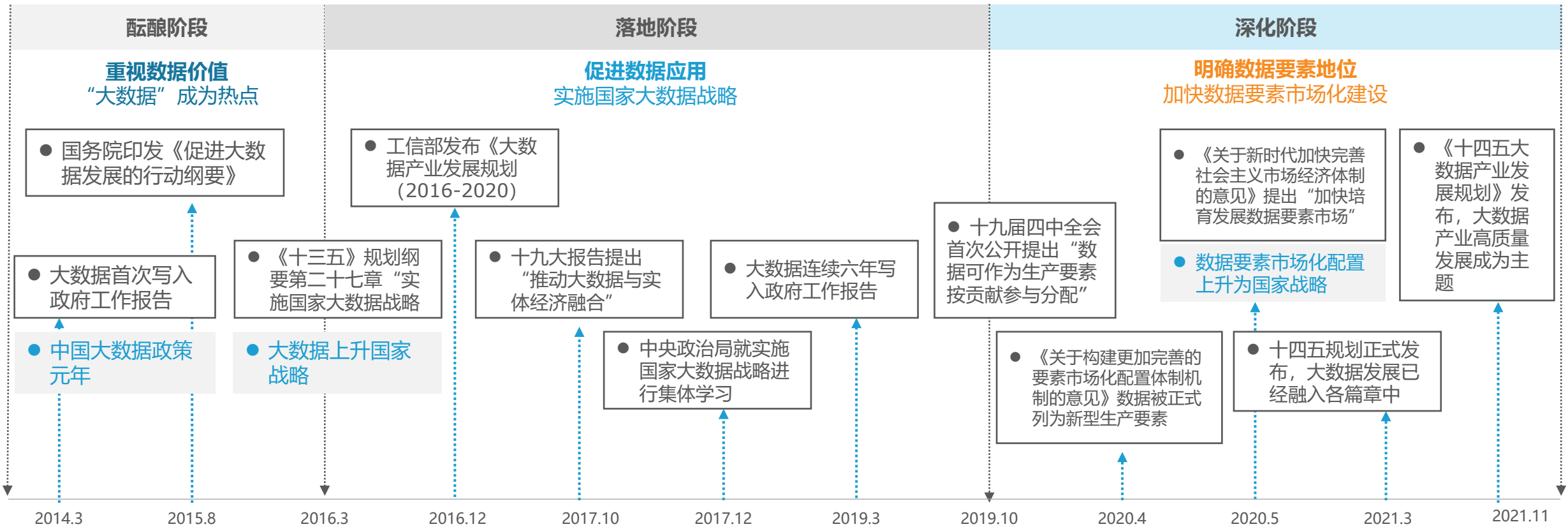
2016年 Google提出了联邦学习在移动互联网上应用的概念，隐私计算技术被认可并进入快速发展阶段。

- J Konecny et 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。

- ◆ 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

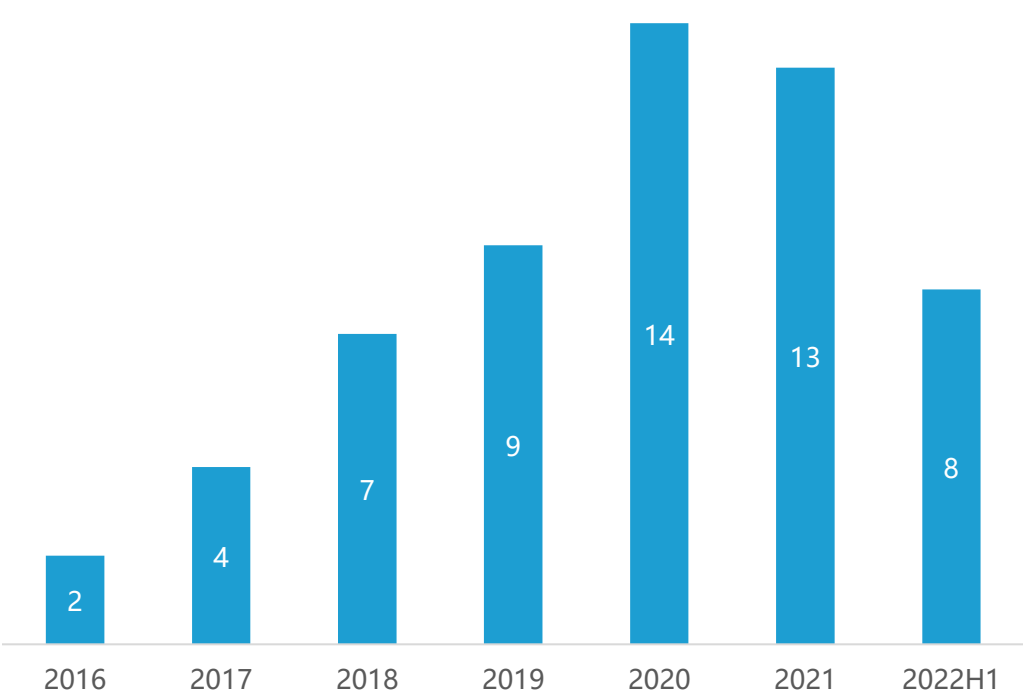
资本市场：隐私计算投融资热度逐年上升

- ◆ 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

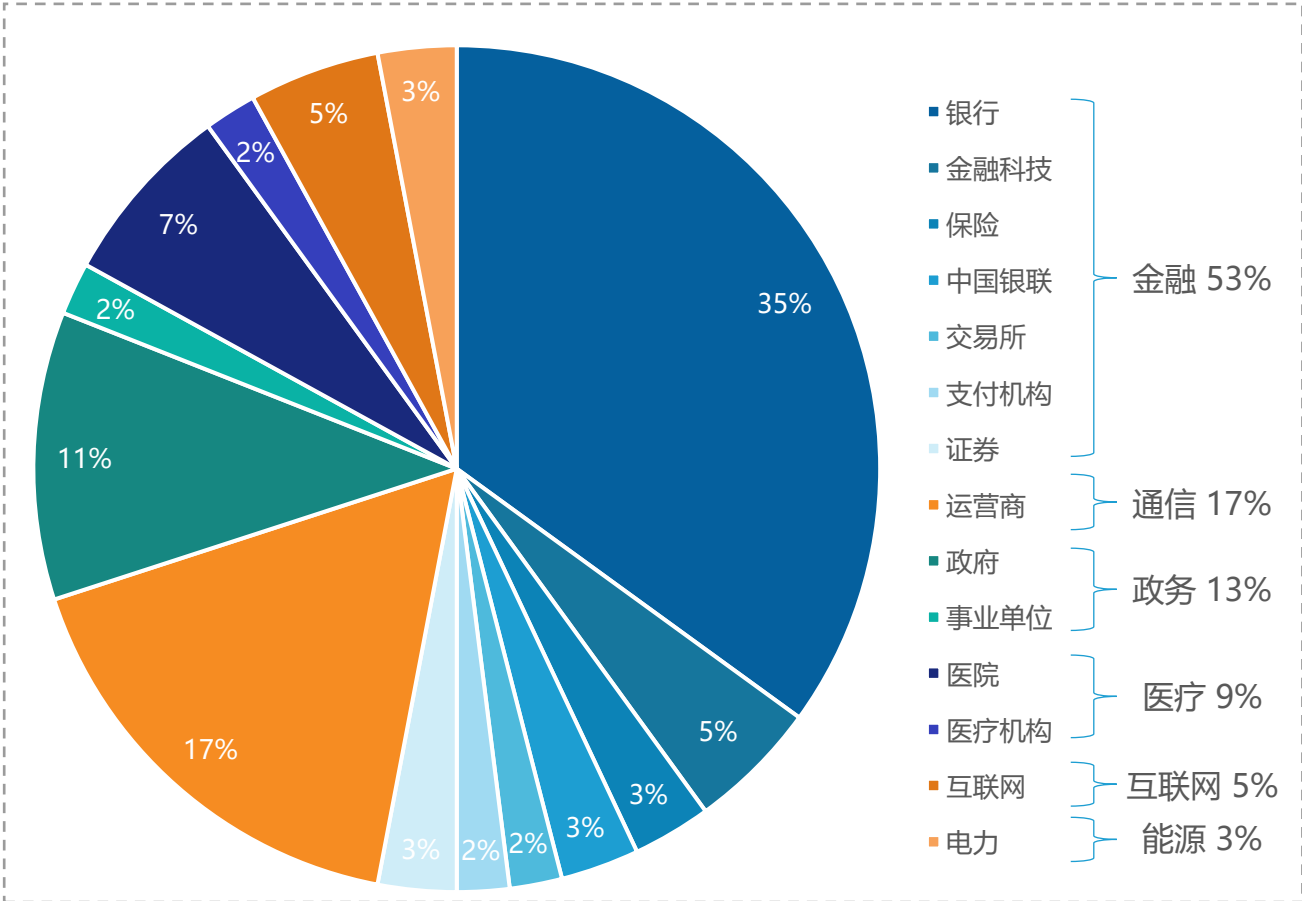
单位：人民币（元）



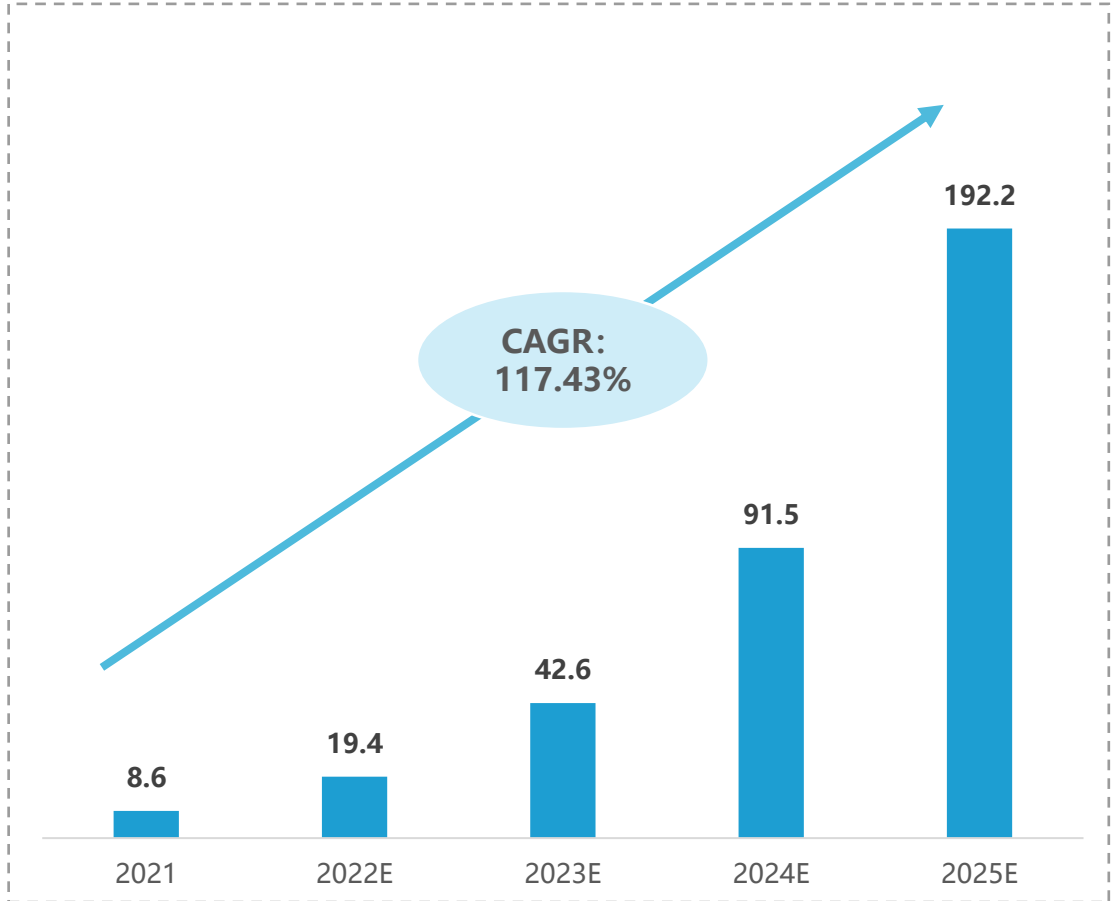
企业名称	投资轮次	融资金额	企业名称	投资轮次	融资金额
数蓬科技	B&B+	约5.5亿	富数科技	C	数亿
宇链科技	A+	数千万	翼方健数	B+	超3亿
洞见科技	Pre A	数千万	冲量在线	Pre A	数千万
趣链科技	C	数亿	锆威科技	B	数亿
星云 Cluster	A+	数千万	同态科技	Pre A	数千万
云象 区块链	B	数亿	华控清交	B	7亿
数泰科技	A	数千万			

- ◆ 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





二、隐私计算产业发展趋势分析

- ◆ **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

◆ 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	OpenMined	多方安全计算、联邦学习
TF-Encrypted	DropoutLabs、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
PaddleFL	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，作为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。

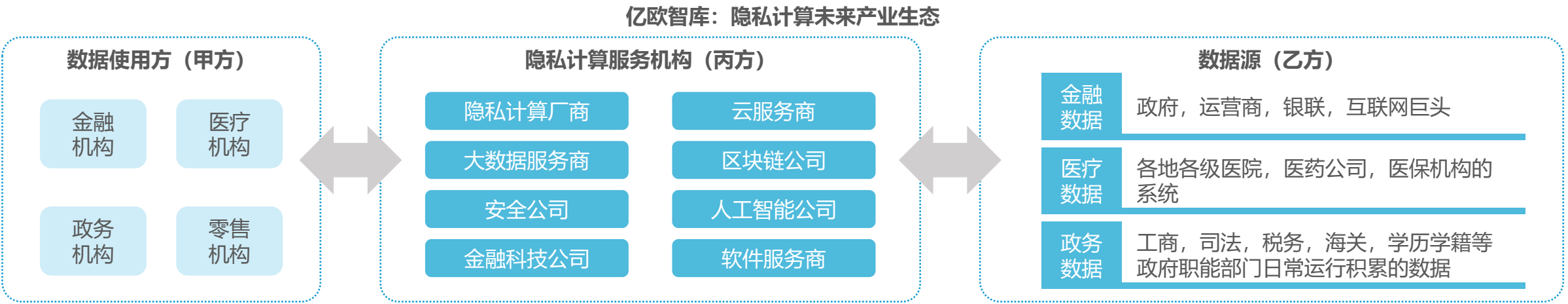
应用

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用阶段，需要产学研用各界加强隐私计算布局。

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，形成既开放又独特的多元生态。

◆ 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。



◆ 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Cluster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

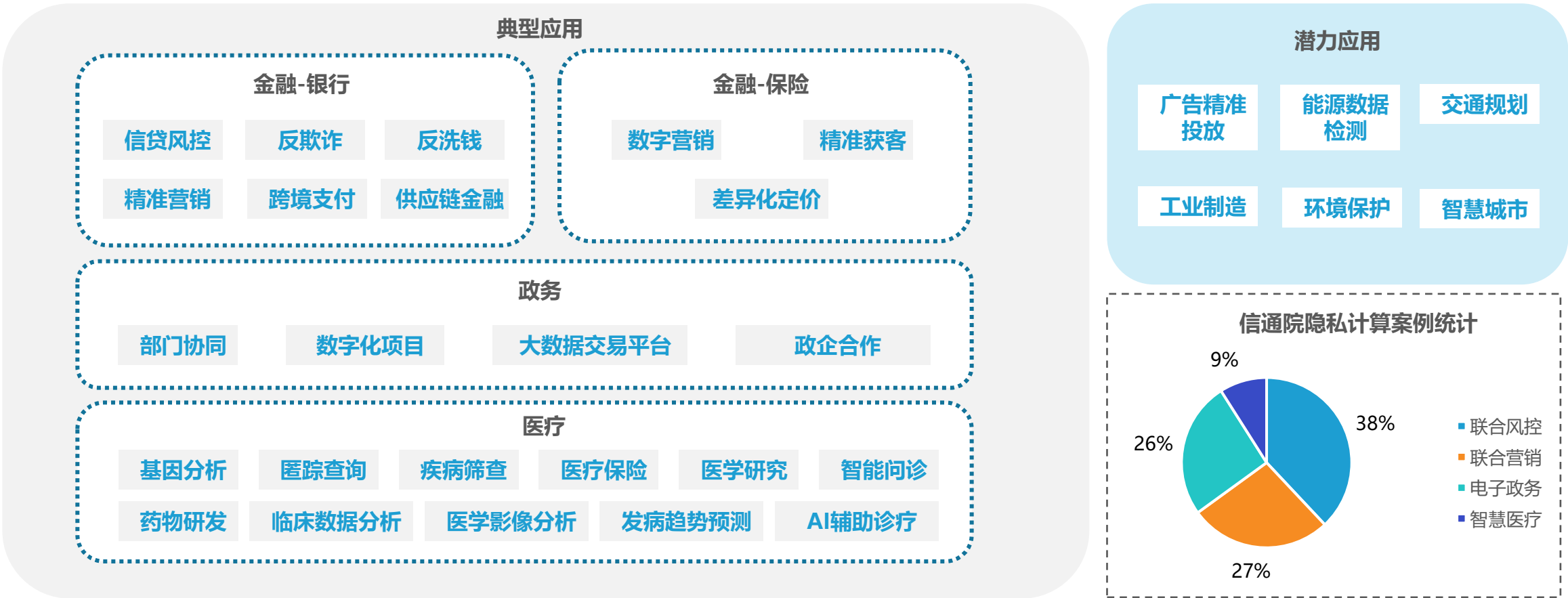


三、隐私计算典型应用场景分析

应用场景：隐私计算的主要应用场景有金融、政务、医疗等

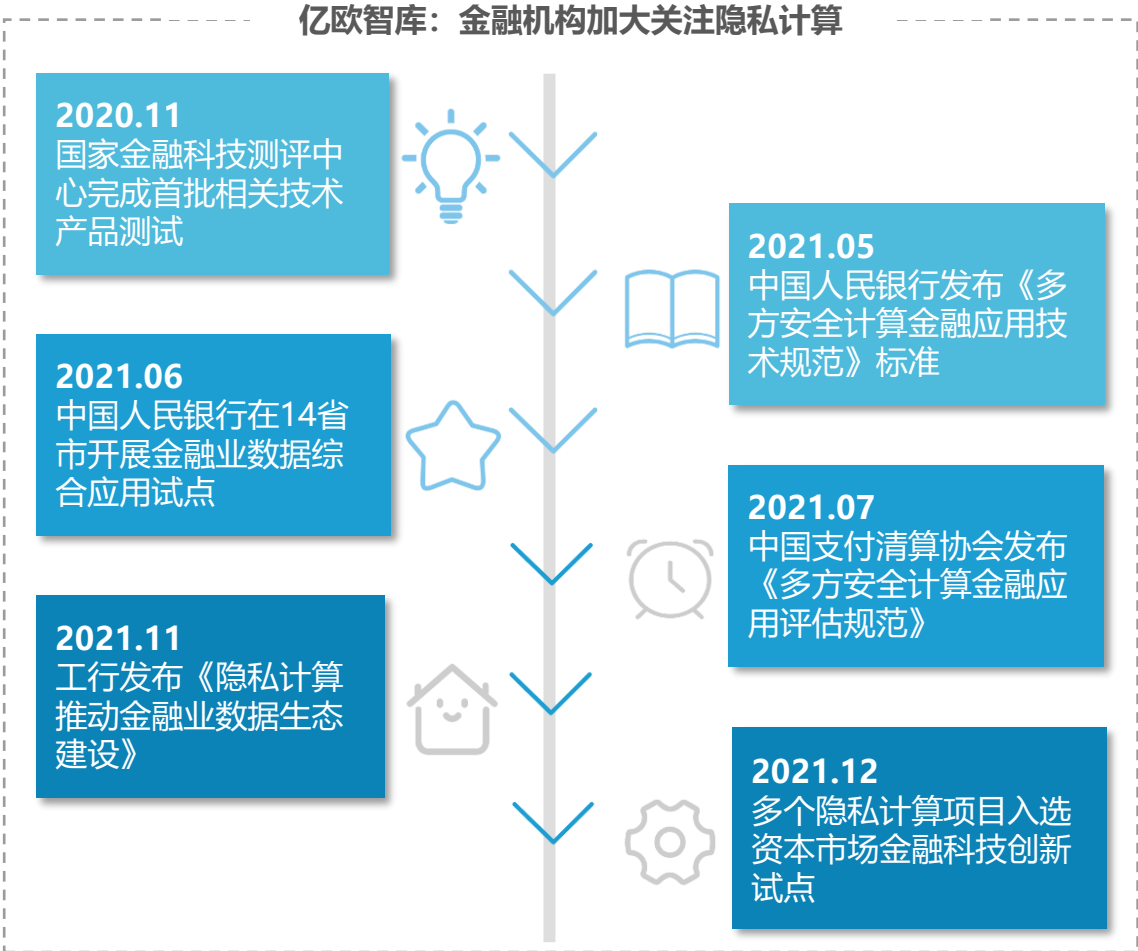
- ◆ 目前市场上隐私计算应用最广的领域主要有金融、政务和医疗，但是蕴含更大经济价值的潜力领域有待更大规模的实际落地应用。
- ◆ **2021年末，金融领域隐私计算应用开始大量落地，预计将在2022年出现爆发。**整体来看，应用最成熟的是银行业、保险业，隐私计算在资管行业发展相对较慢。**政务领域预计将在2022年开始大量投入使用**，短期内主要用于部门协同，数字化项目和大数据平台建设将逐步跟进，经济利益更大的政企合作面临进一步探索。医疗领域的应用相对有些落后，**目前已经有明确的场景和产品，但实际落地的应用较少。**

亿欧智库：隐私计算的主要应用场景

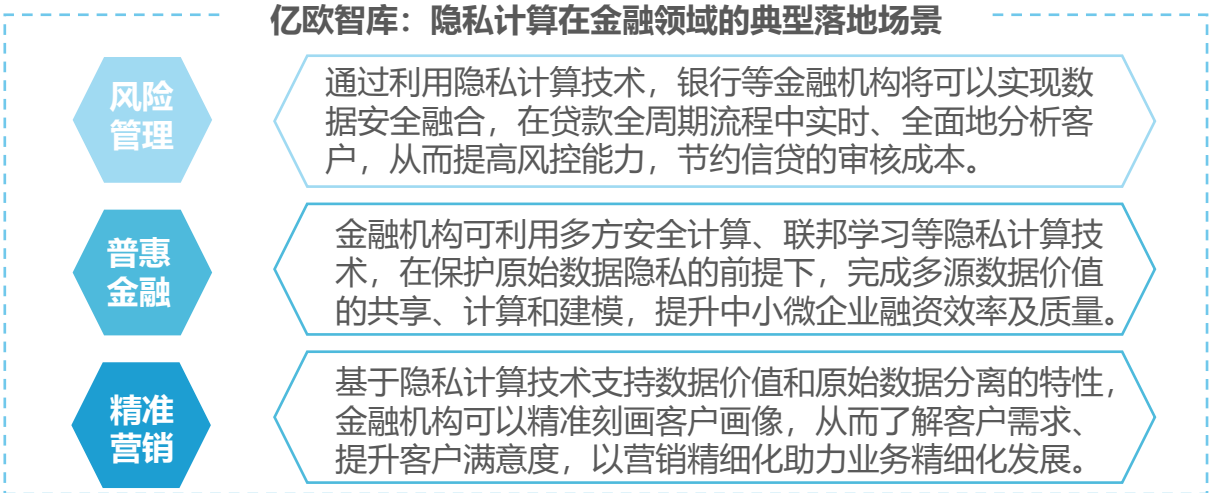
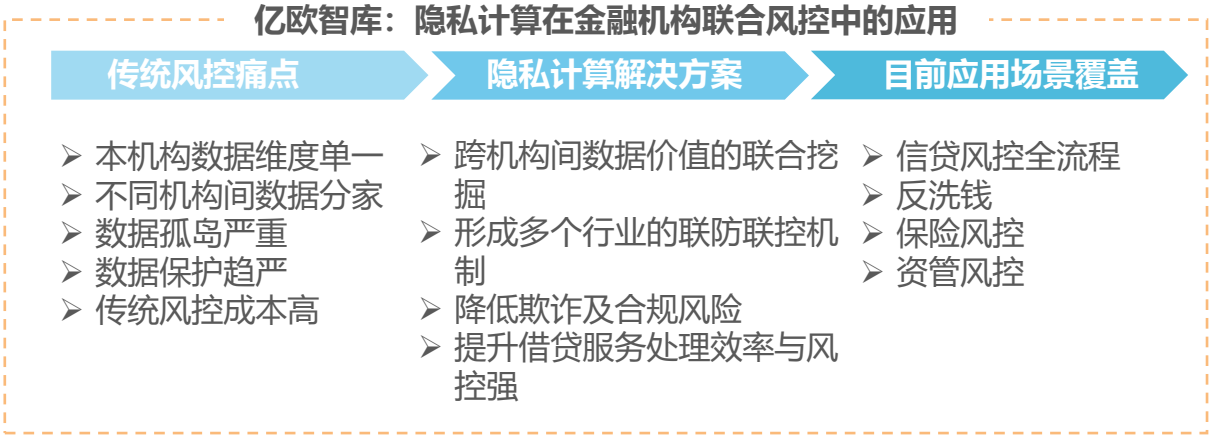


隐私计算+金融：隐私计算应用已较为成熟，风控和获客是两大主要应用领域

- ◆ 金融机构与外部数据源的合作过程中存在的风险主要来源于两个方面：一是涉及大量个人用户信息，受到的监管要求严格；二是机构自身业务积累的数据资产和商业秘密容易泄露。而利用隐私计算，金融机构之间、金融机构同运营商、互联网、电商平台之间等可以在不泄露原始信息的前提下对客户进行联合的精准画像，在信贷评估、产品推荐等场景下有效控制违约风险，提高业务效率。
- ◆ 在金融科技深刻赋能业务的进程中，外部数据的共享应用成为金融机构的强烈需求，金融风控和获客成为目前国内最主要的隐私计算落地场景。



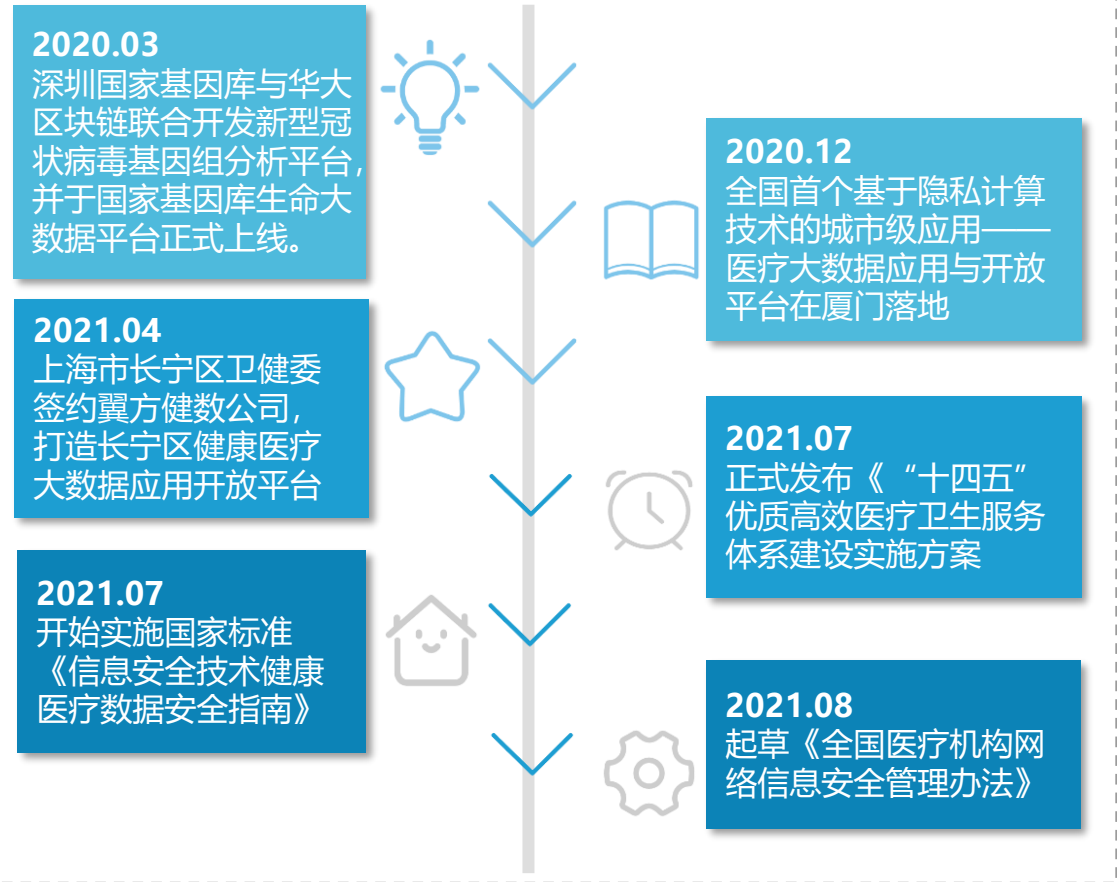
数据来源：中国信通院，公开资料，亿欧智库整理



隐私计算+医疗：隐私计算发展驶入快车道，且受政策环境影响较大

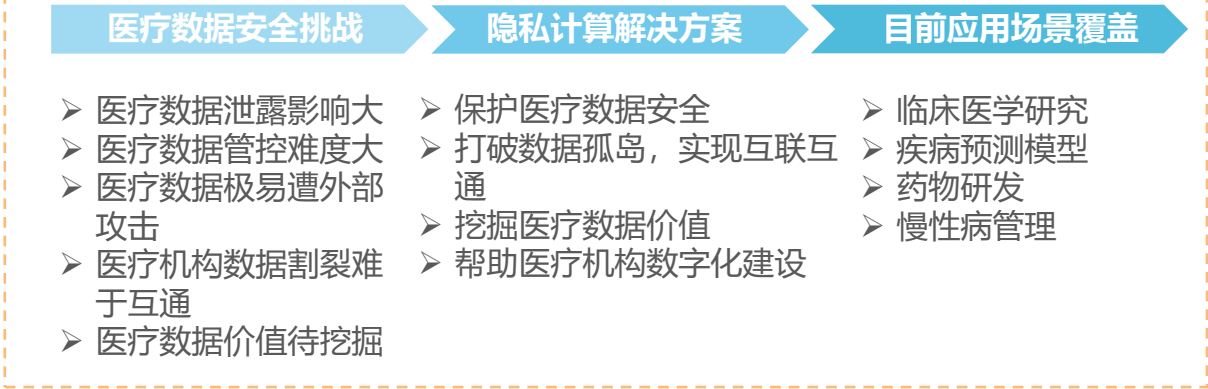
- ◆ 医学研究、临床诊断、医疗服务等对大数据统计分析与应用挖掘有强烈需求，但其依赖的是众多病患的个人健康数据，这些数据规模大、价值含量高，但共享流通困难。利用隐私计算，建立分散存储的标准化数据库，可以实现分布式的联合统计分析，从而获得临床科研的研究成果。
- ◆ 在抗击新冠肺炎疫情的过程中，隐私计算助力实现了全球范围内的疫情数据共享，基于多方安全计算等技术实现了允许用户在不公布己方数据的前提下，联合其他科研人员协同进行病例样本基因组的联合分析并共享结果，成为助力抗疫情的一把利剑。

亿欧智库：医疗数据政策相继出台，实践从概念到落地

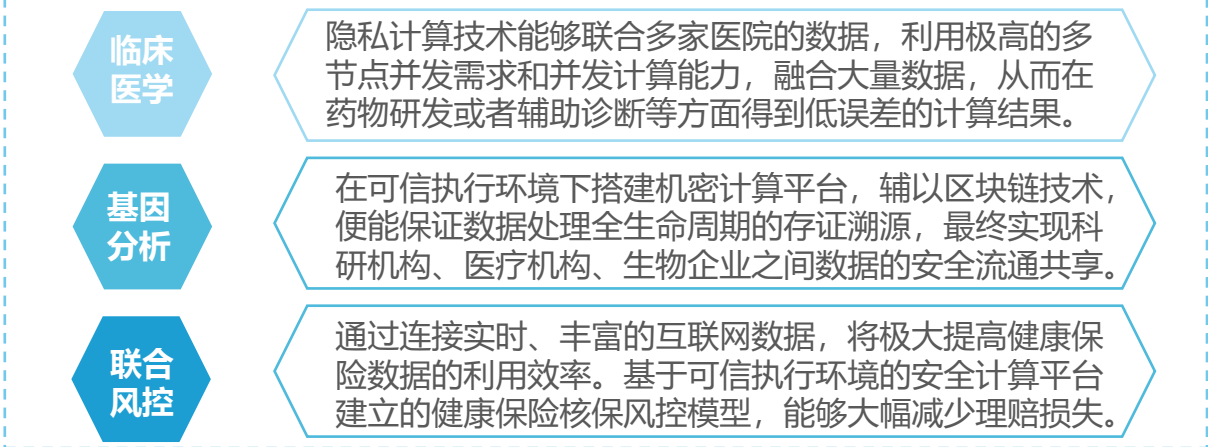


数据来源：中国信通院，公开资料，亿欧智库整理

亿欧智库：隐私计算在医疗数据共享中的应用



亿欧智库：隐私计算在医疗领域的典型落地场景



隐私计算+政务：政务领域场景实践处于探索阶段，省市级创新场景较为突出

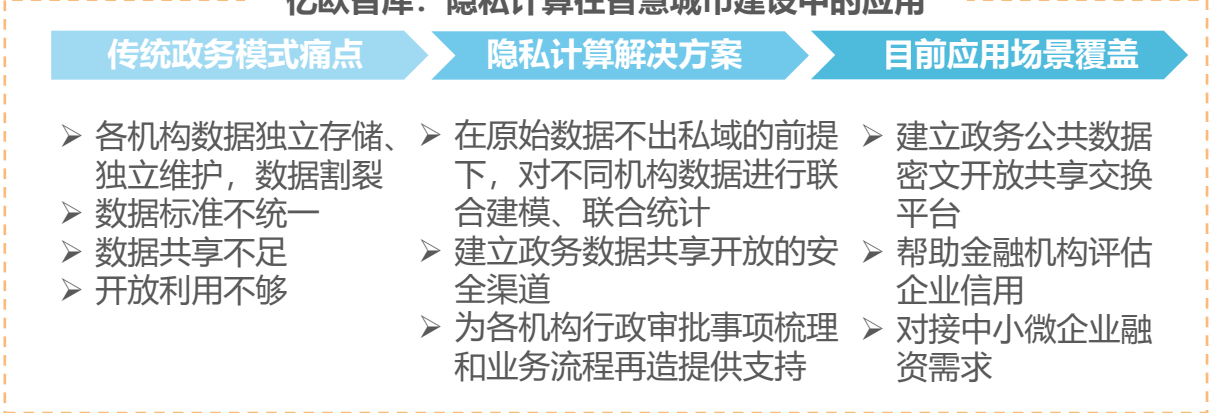
- ◆ 作为跨机构间数据流通的重要参与主体，政务行业有望成为隐私计算技术落地的下一个重要场景。政务数据的规模大、种类多、蕴含价值高，涉及公安、交通、税务、环境等各类人民生活和社会运行的数据，政务数据的流通与应用将释放巨大能量。
- ◆ 各地政府积极推进政务数据的开放共享，但不同部门之间的数据孤岛难以快速消除，且政务数据涉及社会民生，数据合规和安全管控要求更加严格。因此，隐私计算为此提供了解决方案，在跨机构之间的个人身份确认、企业经营监管、智慧城市建设等众多场景中均有广阔的应用前景，且在部分地方政府的相关规划里，已经有所涉及。

亿欧智库：政务数据实践案例显著增多

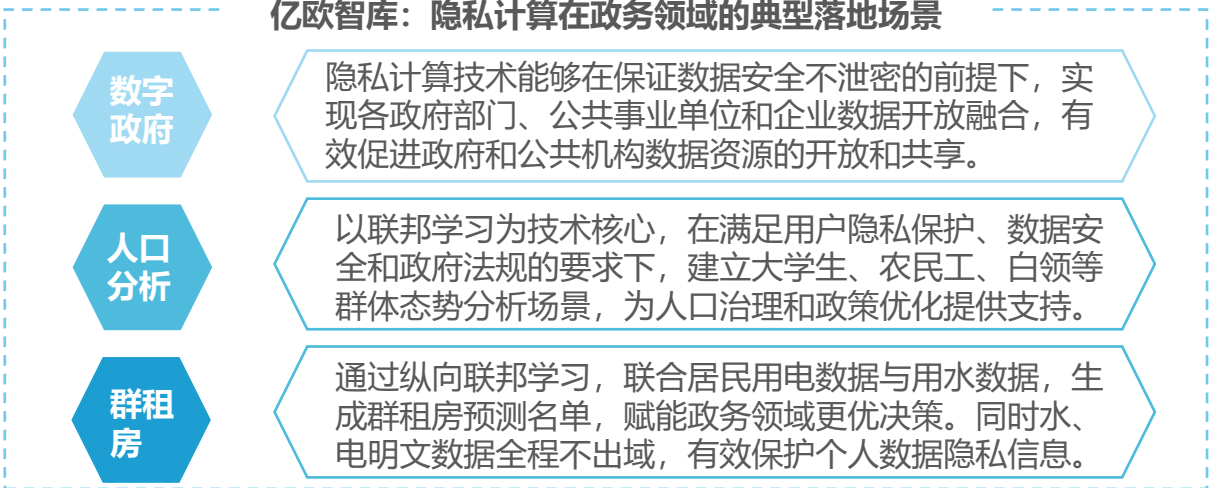


数据来源：中国信通院，公开资料，亿欧智库整理

亿欧智库：隐私计算在智慧城市建设中的应用



亿欧智库：隐私计算在政务领域的典型落地场景



行业先锋：隐私计算二十大技术领先企业榜单（按拼音首字母排序）



百度



京东云



诺威科技



天冕科技



星云Cluster



百融云创



矩阵元



融数联智



同盾科技



翼方健数



洞见科技



蓝象智联



数牍科技



微众银行



翼支付



华控清交



蚂蚁集团

腾讯



星环科技



字节跳动

百融云创——SaaS云服务金融数智化赋能者

- ◆ 百融云创成立于2014年3月，2021年3月在香港主板成功上市。作为中国金融行业数智化发展优质合作伙伴，百融云创**独立研发的SaaS云突破性运用人工智能、云计算、区块链和机器学习等技术，为金融行业提供高适配性的产品及解决方案**，实现全面赋能，并基于长期的行业理解和洞察，帮助合作机构完成数智化转型。
- ◆ 凭借出色的前沿技术和数智化能力，百融云创与六大国有银行、十二家全国性股份制银行、上千家城市商业银行和农村商业银行，金融科技公司、消费金融公司、汽车金融公司、保险公司等**超6000家金融机构**达成合作并提供专业服务。

2014

生于瓦砾

2013年，互联网金融萌芽，创始团队开始尝试将人工智能和数据要素结合，应用于金融领域。百融在2014年应运而生，标志着智能科技在金融行业应用的正式起航。

2015

灿若夏花

2015年，百融拿到了B轮融资，签下招行、光大等合作伙伴；建立人工智能实验室，综合应用场景成功拓展到消费金融、小微金融及保险、基金等金融场景。

2019

宛若黎明

2019年，行业规范及洗礼加速，对金融科技企业提出了更加严苛的要求。百融始终保持战略前瞻性，以合规发展作为战术要求，不断梳理和迭代业务线条。

2022

未来有你

展望2022年，百融将持续加大前沿科技在金融领域的布局，夯实技术创新优势，并通过精细化管理和运营降本增效。

百融云创服务矩阵



智能分析与运营服务

百融云创以人工智能、云计算等核心技术为基础，协助金融机构构建智能分析体系，通过多维分析辅助决策，提升决策的准确性；通过精准的客户画像，提升客户分类管理和目标市场识别能力，提升策略匹配和客户价值。



精准营销服务

百融云创通过专有金融产品推荐平台为金融机构提供精准营销服务，使其能更有效的触达及服务目标客户。百融云创通过人工智能和云计算等核心技术的赋能，经过营销意向模型筛选出高意向客户，匹配场景灵活调整运营手段，配置多种耦合运营策略，最终将用户与合适的金融产品匹配。

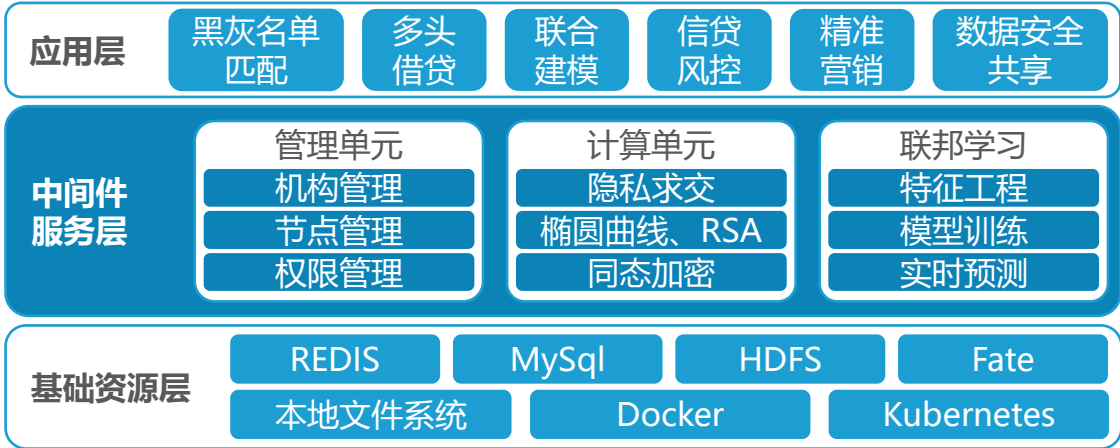


保险营销服务

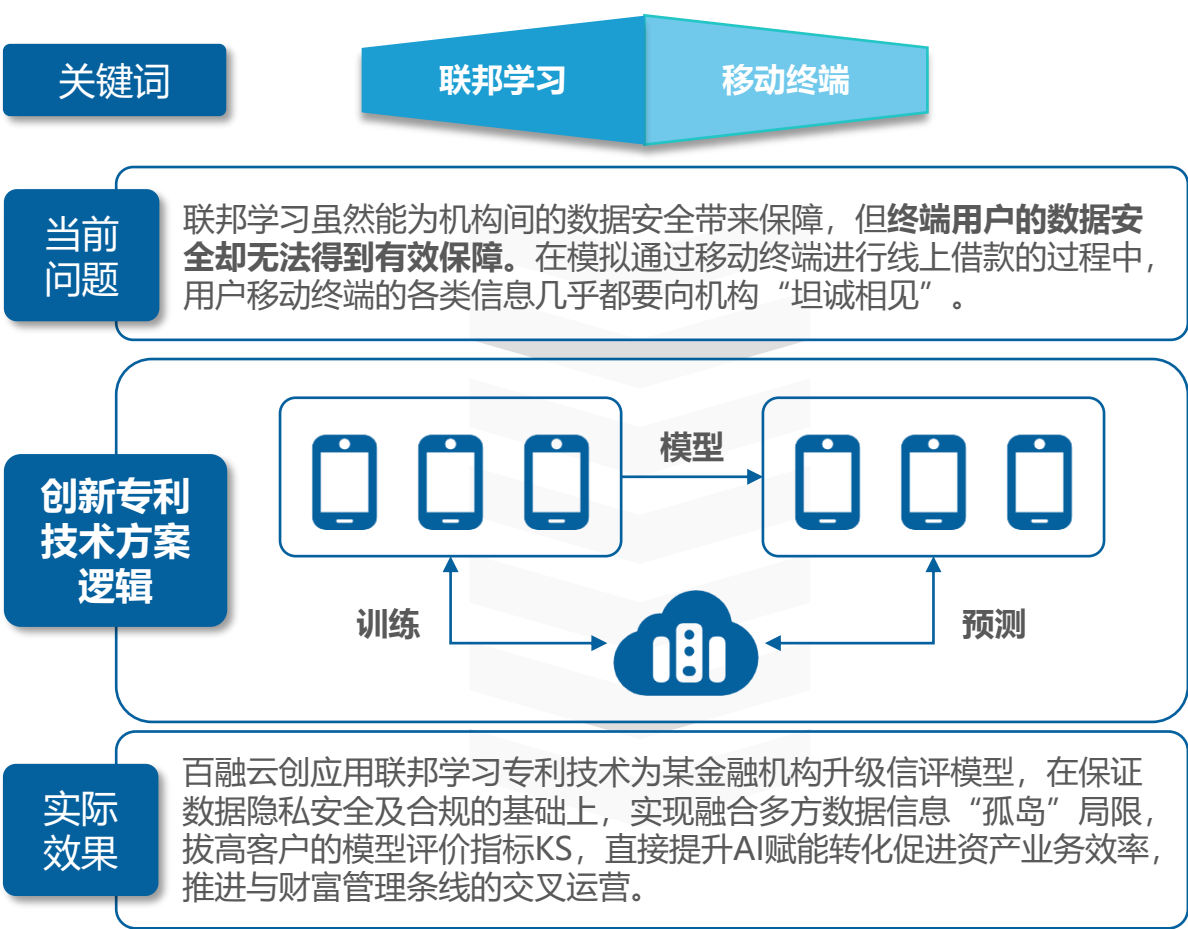
百融云创透过黎明科技平台提供保险分销服务，为经纪人提供数据驱动及分析工具，使经纪人更好地评估消费者，保障消费者需求与保险产品精准匹配，并透过实时管理移动化工具平台，以改善经纪人的销售及留存表现。

- ◆ 政策驱动、市场催生、技术引导三股力量驱动着“隐私计算+”时代到来，百融云创搭建隐私保护计算平台Indra，为金融数据应用过程中保障数据可用性和隐私性给出了创新解法。
- ◆ 用户使用移动终端，不可避免地会在多个环节都存在个人隐私泄露的隐患。百融云创一项联邦学习国家发明专利授权“一种基于联邦学习的移动终端信用反欺诈预估方法及系统”受到业界关注，这项技术将从底层逻辑上化解“隐私交换便利”的困局。

百融云创Indra产品技术架构

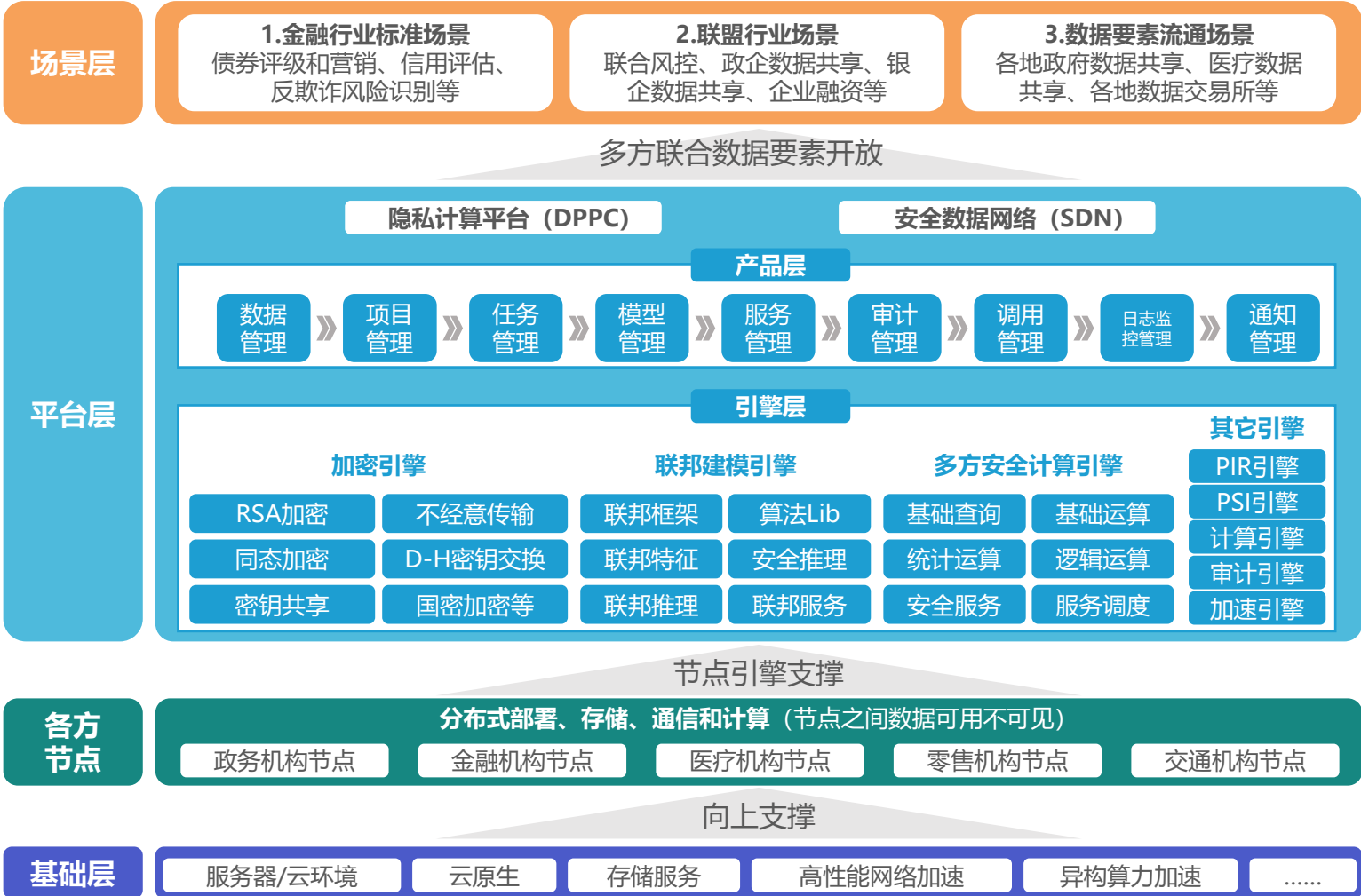


基于联邦学习的移动终端信用反欺诈预估方法及系统



◆ 星云Cluster是一家**以算力为核心**的隐私计算技术提供商，专注于**高性能隐私计算算力产品**研发与技术创新。公司产品包括隐私计算的软件计算平台，软硬一体机、算力加速卡以及芯片等。致力于以“算力+”技术布局与战略理念，为隐私计算应用规模化落地打造算力“基建”，高效赋能数据有序共享与综合应用。

星云Cluster产品架构



星云Cluster技术背景

181项

隐私计算、联邦学习
专利申请数量

No.1

隐私计算算力核心专利申请
量与授权量赛道第1

星云Cluster服务案例

金融

国有大行隐私计算平台
依托隐私计算平台能力
搭建联邦学习多方安全建模平台

汽车

某知名汽车数智化服务商
依托隐私计算平台联邦学习能力
搭建多方安全建模精细化运营平台

AI

某知名人工智能软件公司
RDMA虚拟化网络实现
高性能网络下的多租户管理

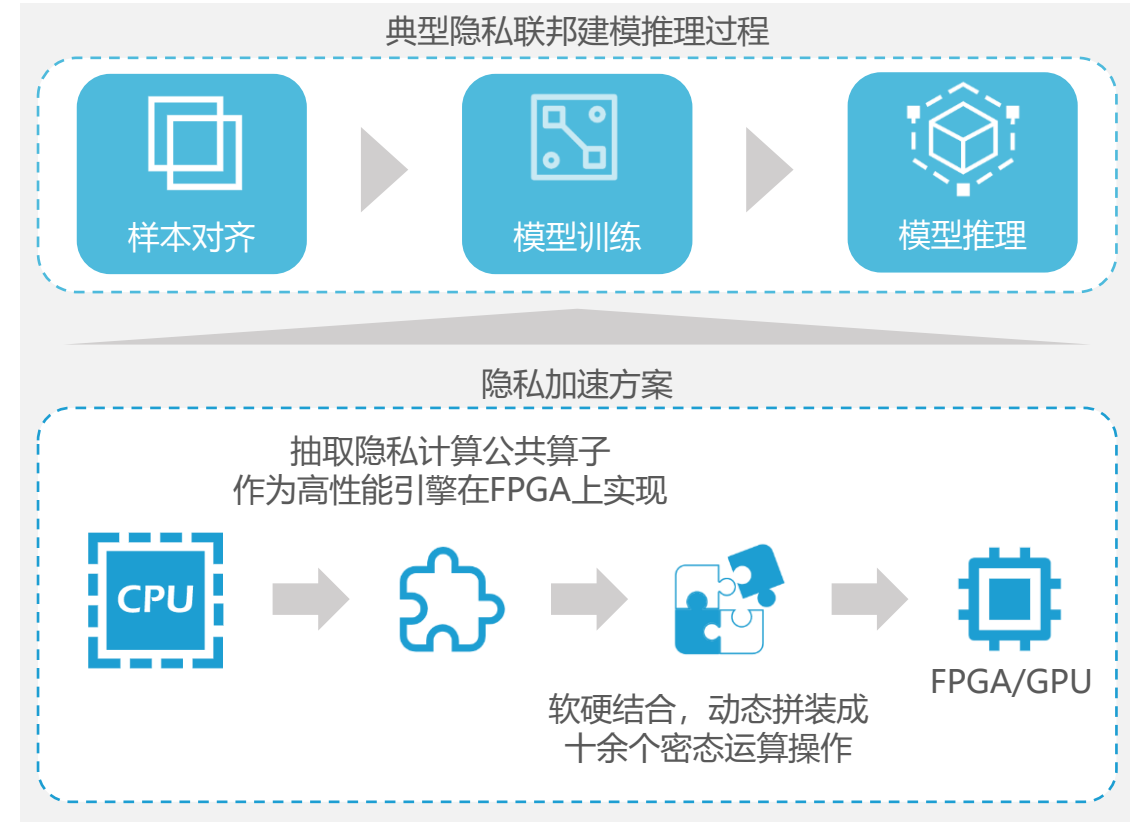
医药

某知名医药企业
依托隐私计算平台能力
实现联邦视觉任务

业界首款硬件异构算力加速方案助力头部互联网银行效率提升

◆ 基于在高性能数据中心、网络通信等领域的深厚研究，星云Clustar推出了业界首款硬件异构算力加速方案与FPGA算力加速卡。该方案采用星云Clustar自主设计研发的多任务并行、多引擎架构，支持GPU和FPGA加速，能够灵活加速多种类型的加密工作负载，大幅强化分布式隐私计算的通信效率与计算能力。

解决方案逻辑图



70% 功耗降低

10倍 性能提升

300% 延迟降低

数据来源：星云Clustar官网，亿欧智库整理

某头部互联网银行信贷场景纵向联邦学习项目

项目背景

星云Clustar为某头部互联网银行定制了基于NVIDIA GPU和Xilinx FPGA的联邦学习异构加速方案，通过GPU+FPGA的算力，大大地提升了联邦学习整个端到端的计算性能。

系统加速方案

FATE联邦训练流程和基本的数据源抽取由CPU控制，训练过程中的数据计算则下发到FPGA和GPU来承担。
FPGA主要负责同态加密计算，密文矩阵运算，密文乘法运算，模幂运算。GPU主要负责同态解密运算，密文求和运算，数据混淆运算，密态加法运算，模乘运算等其他运算。
实际工作中，FPGA和GPU是独立且并行工作的，能同时进行GB级别的大数据量运算，且FPGA和GPU单个芯片也分别支持多任务并行执行计算。

实际效果

在实际场景中，数据量超过1千万个级别，数据特征维度超过30维，进行FATE纵向联邦训练，加速效果为端到端相对于CPU多核提升3倍，单核提升平均为60倍。

	参与方1数据量和维度	参与方2数据量和维度	CPU计算耗时-16核	FPGA+GPU计算耗时	20核性能加速比	单核性能加速比
XP-LR	1000万×10	1000万×30	0:39:52	0:10:38	3.75	60
使用硬件说明	CPU：Intel(R) Xeon(R) Platinum 8163 CPU @ 2.50GHz 16 Core GPU：Nvidia V100 FPGA：Xilinx VU13P					

翼方健数——以全栈技术塑造“数据与计算互联网”

- ◆ 翼方健数以隐私安全计算为核心，为医疗、金融、政务等行业建设在数据安全和个人隐私保护基础上的数据开放生态和数据共享协作环境，并在此基础上发展人工智能的能力，为行业赋能。
- ◆ 翼方健数针对数据跨域流通全流程提供一套全栈的解决方案。通过自主研发的隐私安全计算平台翼数坊XDP实现数据分享和价值获取的平台能力，核心模块包括分布式文件系统XFS、计算资源调度与适配引擎XEE、高效的数据发现与整合模块DaaS以及为不同信任假设场景储备的安全计算技术路径PCT（支持包括MPC，FHE，联邦学习，TEE等多种计算环境），利用全栈技术产品保证数据隐私和安全的同时，解锁数据价值。

翼方健数解锁数据价值的全栈技术矩阵



翼数坊XDP平台具备三大核心能力

- 1 数据全生命周期管理
- 2 坚实的隐私安全计算技术体系
- 3 数据驱动的差异化AI应用

翼方健数不仅把自己定位成一个隐私计算的公司，更定位是一个**实现数据价值的公司**，其中隐私计算是非常重要的一个手段。我们在技术发展上是全栈式的，对多方安全计算、联邦学习、可信执行环境等技术都有很大投入。翼方健数有一个更强的能力，就是我们知道在某种情况下，应该用哪些技术组合以获得最好的效果。

——翼方健数首席科学家 张霖涛

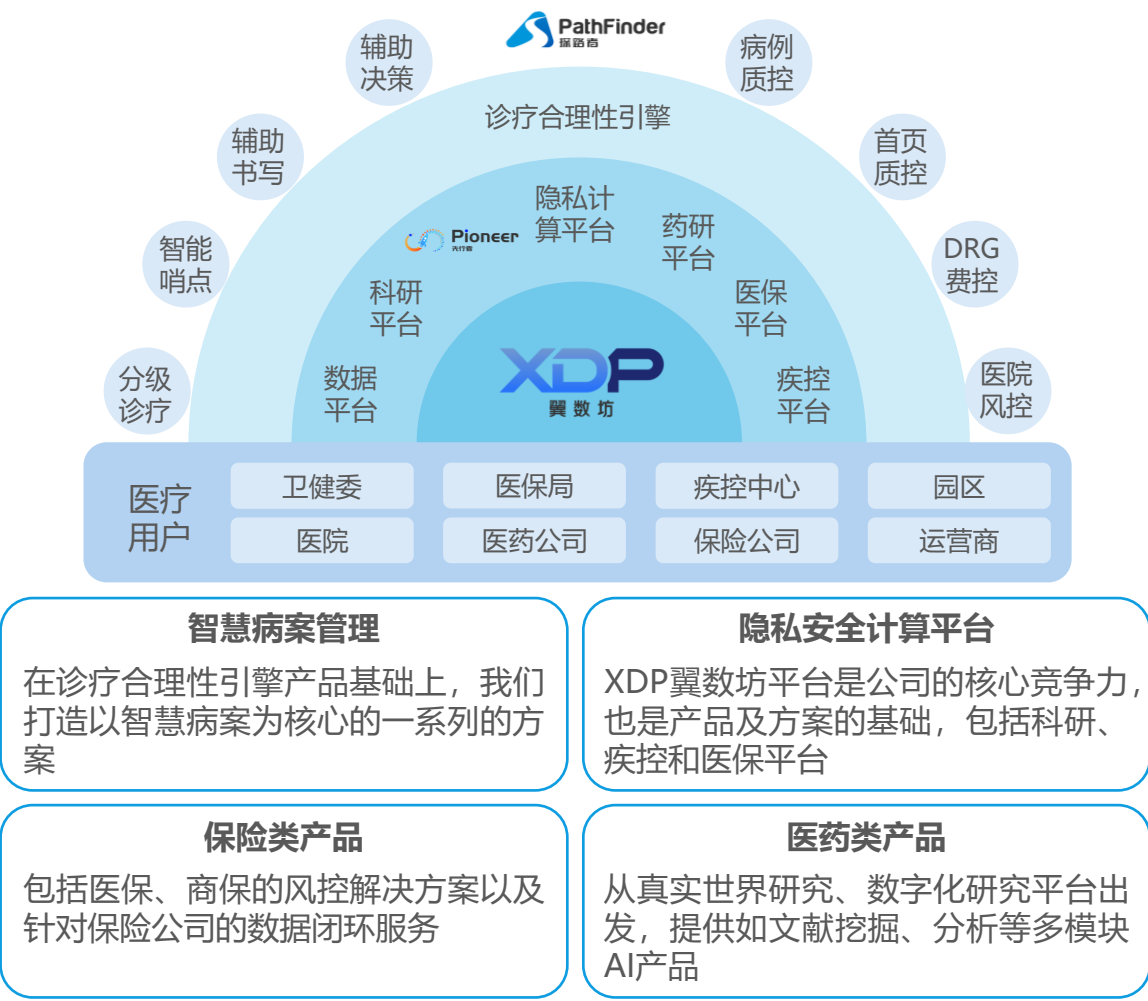
建设IoDC网络的两大基石

- 1 平台是实现智能应用的基础
- 2 智能应用帮助IT基础设施得以进步和完善

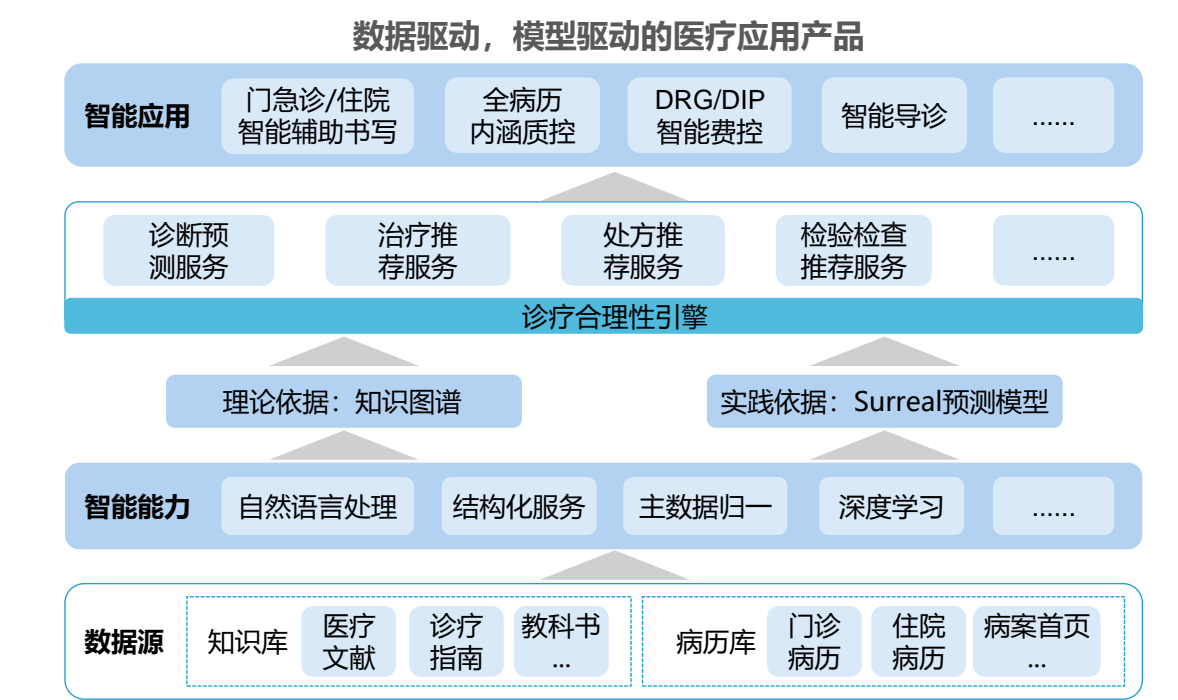
- ◆ 翼方健数提出基于隐私安全计算的“数据与计算互联网（IoDC，Internet of Data and Computing）”，作为数据原生时代**新一代的IT基础设施**来应对各种挑战。翼方健数已成功实现**区域或行业XDP联盟**（IoDC雏形），实现数据价值，让每一个节点能够从中获利，通过商业价值来促进数据所有者，数据使用者和数据服务者之间的协作运行。

翼方健数基于隐私计算与人工智能能力在医疗领域实现数据闭环

◆ 在医疗健康领域，翼方健数通过以隐私安全计算为核心的人工智能全栈解决方案，服务于各地、市级卫健委大数据中心的数据资产化管理以及疾控预警预测，还有各三甲医院院内基于大数据安全应用的科研平台、智慧病案等。



◆ 医疗机构间的数据共享与流通需要隐私计算网络作为基础设施。目前翼方健数为实现从数据-能力-模型-应用的全流程医疗数据价值闭环，通过智能技术收集、处理、分析、训练模型，最后通过智能应用将数据落地、沉淀，作为建立隐私计算网络的基础。医疗机构在自己充分发掘数据价值的前提下，作为供应方将数据共享，以获得更多收益。



典型客户

上海交通大学医学院附属瑞金医院

厦门市健康医疗大数据中心


宜昌市卫生健康委员会

四川大学华西第二医院

数据来源：翼方健数官网，亿欧智库整理

- ◆ 星环科技致力于打造企业级大数据基础软件，围绕数据的集成、存储、治理、建模、分析、挖掘和流通等数据全生命周期提供基础软件与服务，构建明日数据世界。
- ◆ 星环科技旗下的Sophon P²C是**国内首批通过信通院资质认证的隐私计算平台**，集隐私计算、加密网络通信等多种功能，为多方数据写作提供完整的解决方案。以隐私保护为前提，**Sophon P²C解决了跨组织协作时无法安全利用各方数据的困境。**
- ◆ Sophon P²C拥有以下**四大优势**：

权威认证 有效保障客户数据安全	计算框架多元化 面向全行业落地
分布式框架 个性化联邦学习建模	良好的系统稳健性 灵活的部署方式



伊人
星环科技隐私
计算科学家

我们的核心优势可以归结如下方面：第一是**星环品牌的优势**，我们在整个数据行业已经拥有很多成熟的案例和深厚的行业积累，对数据本身的理解和对软件的理解很深。第二我们对**各个行业的业务有自己的积累**，我们在这方面有比较多的战场。第三是我们的隐私计算拥有较多的安全认证和**较强的技术能力**，能够取得客户的信赖。第四我们在**商务上也有很多的合作伙伴**。这些是星环的外围能力，从技术上来说，我们提供了一整个链路式的数据隐私保护，拥有很高的**数据安全防护能力**。

数据来源：星环科技官网，亿欧智库整理

星环科技群租房智能分析项目

项目背景

“基于用电信息采集系统的群租房智能分析” 排查方案：通过研究发现群租房用户的用电规律和用电特征等问题，并有针对性地提出可行性的应对策略，为深入解决“群租房” 问题提供理论基础。

客户痛点

- “**进门难、认定难、执行难**”：检查高峰期执法人员难以进门；每次短时间执行后，又将面临群租反弹
- **行政执法与群租群体矛盾突出**：当政府资源无法跟上群租问题的同步增加时，政府在对待群租问题时变为一种“选择性执法”
- **群租房具有隐蔽性**：群租房皆是用于生活，除非租住其中或者是周围邻居举报，否则难以发现

解决方案

- 整体建设思路：基于星环TDH大数据平台接入多源异构数据后，使用**星环Sophon智能分析工具**，通过从海量用电数据中提取用户特征、采集并分析租房信息、基于地理位置信息匹配分析、群租房用户识别建模等步骤后，将模型预测出的部分群租房用户地址映射至地图。
- 在本项目中，为提升识别效果，除分析用电数据外，还引入了水务部门的用水数据，基于Sophon P²C隐私计算平台进行纵向联邦学习

主动方

用电数据

数据处理

用电特征+标签

主动方联邦学习平台
协调方联邦学习平台
参与方联邦学习平台

参与方

用水数据

数据处理

用水特征

水电数据
联邦学习
模型

生成
可疑
名单

实际效果

- 将模型预测出的部分群租房用户地址在地图上映射，经过线上对模型的测试以及线下对预测地址的核查，**准确程度超过九成**
- 模型效果方面，单独用电模型的AUC（识别准确率）仅为73.49%，而使用水电融合模型精度达到91.21%，**可见使用纵向联邦学习安全地引入更多分析维度后，模型效果提升了24%**

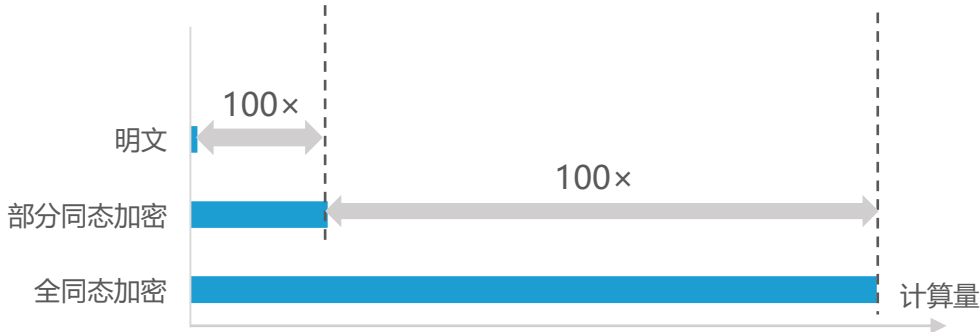


四、隐私计算产业发展机遇与挑战

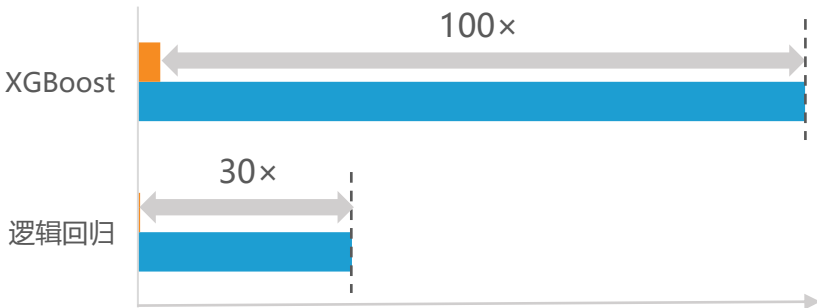
隐私计算发展目前存在性能瓶颈，下游用户面临性能与安全间的平衡选择

- ◆ 相比明文计算，密文计算对算力与通信负载的要求更高，相同内容的明文与全同态加密的计算量可相差四个数量级。隐私计算的高计算量对设备性能提出高要求，目前技术环境中易遇到性能瓶颈，除了算力算法层面需要优化外，通信效率与通信压缩技术也需要进一步提升。
- ◆ 根据外部测试结果可见，40万行样本×900列特征的纵向联邦学习建模平均耗时比明文慢数十倍甚至百倍，随着数据规模增加，差距还会继续被拉大。

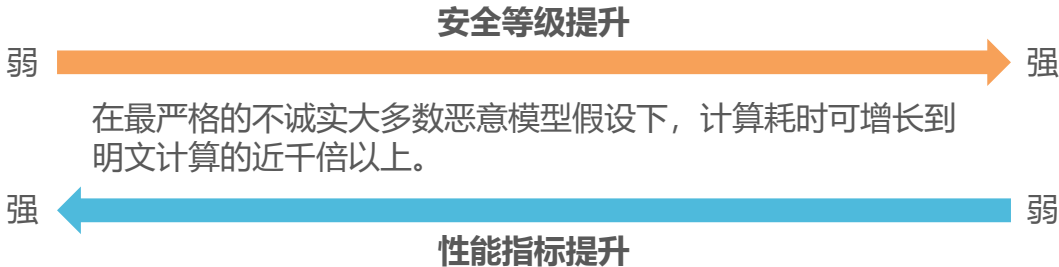
同态加密计算量对比示意图



纵向联邦学习平均耗时示意图



- ◆ 随着安全性和隐私性提升，隐私计算的性能通常会出现下降。根据中国信通院“可信隐私计算”性能专项评测以及对一些相关论文的结果，安全假设较弱时，其性能普遍较强；反之，安全假设较强时，其性能普遍较弱。
- ◆ 在实际的业务场景中，行业用户需按需选择，应根据实际需求选择适合的安全等级，实现安全与性能的动态平衡，避免唯安全论/唯性能论。



问题的实质是在数据安全和数据处理的效率之间的平衡选择。特别是国内市场的行业用户侧，对合法性和隐私保护的认知程度，与发达国家存在很大差距。国内企业更加讲求时效性，所以当新技术尤其是围绕数据安全的技术出来的时候，大家其实默认的第一选择都是要保证业务效率。

但从一个长期的发展来看，我觉得牺牲1%的业务效率，使数据安全性得到了指数级增长，对业务可持续性大有帮助。


——某隐私计算垂直厂商行业专家

隐私计算产品本身安全性仍有进步空间，一定程度上制约其推广应用

◆ 隐私计算产品出现的意义在于保护隐私数据的安全流通，其本身的安全性不言而喻。算法协议安全性不足、开发应用安全性不足和安全共识难以达成是当前隐私计算面临的三大安全性挑战。

1

算法协议
安全性不足




隐私计算产品的算法协议差异化较大，各类技术路径所依据的理论基础来源不同，难以形成统一的算法安全基础。

	多方安全计算、同态加密等	联邦学习	可信执行环境
主要协议安全基础	数学与密码学基础	机器学习理论	硬件安全技术

隐私计算产品安全协议依赖安全假设（比如假设硬件提供商的可信性、计算参与方会遵循协议流程、多个参与方之间互不共谋等），以此为基础进行协议和算法的设计，但假设的深度和广度需要时间经验来扩充沉淀。

2

开发应用
安全性不足



隐私计算产品在设计开发过程中易遭遇多种数据安全攻击，如密码学算法通常遇到的侧信道攻击、错误注入攻击，硬件通常遇到的侵入式攻击，或者类似其他信息系统遇到的恶意黑客攻击。对于隐私计算产品的要求是在整个计算的过程中保证绝对安全，而“木桶效应”会导致最薄弱的环节成为产品最易被攻击的部分。

第三方机构的介入也会引来安全风险。在实际使用中，诸如证书管理中心等任何第三方机构的介入，有可能打破技术信任的完整性，引入不确定的风险因子。

3

安全信任共识
难以达成

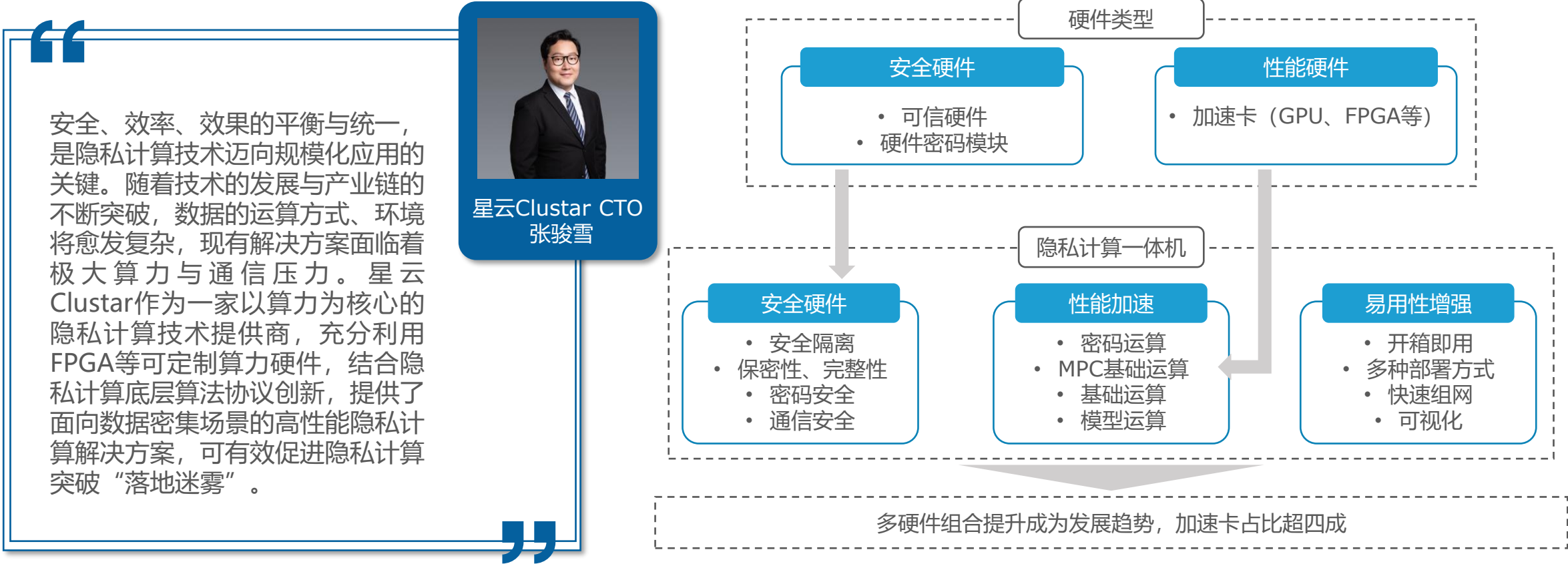
隐私计算涉及较多隐私保护技术与算法，在多个数据参与方共同参与协同计算过程中极易对各不相同的算法逻辑无法达成共识。算法的复杂度、性能与优势场景存在一定差异，隐私计算参与者难以通过直观的方法验证所用产品的安全性。目前隐私计算行业内缺乏有代表性的产品系统性安全分级标准。而现实中各方参与者难以达成信任共识将会延缓隐私计算技术的部署和发展。

数据来源：公开资料搜索，亿欧智库整理

33

软硬结合的隐私计算一体机将会成为行业主流产品形态

- ◆ 当下，利用硬件特性增强软件功能，将复杂的运算移至其他硬件设备来执行，可大幅提升并行处理效率，支持高并发、低延迟，是实现隐私计算性能和安全性同时提升的主流方法。越来越多的行业用户开始关注软硬结合的隐私计算解决方案。行业用户最初主要偏向于采购以软件层面的解决方案，但是由于性能瓶颈所导致的安全风险逐渐显露，行业用户开始寻找其他更优质的解决方案。
- ◆ 隐私计算一体机作为软硬结合一体的专用设备，其安全加固、性能加速和易用性增强的三大优势，使得隐私计算一体机从众多工程优化方案中脱颖而出，降低用户使用技术门槛和综合成本。当然并非仅有隐私计算一体机可以突破应用瓶颈，如FPGA算力加速卡、异构算力加速等软硬结合的多种解决方案，也对扩大隐私计算应用规模起到积极推进作用，但仍需进一步探索，加快场景落地。



◆ 隐私计算落地后的最大功能之一便是推进跨机构数据流通，而由于产品间技术基础、算法逻辑等各不相同，设定行业标准、建立行业共识成为当务之急。其中提出的互联互通基础原则为：保证各隐私计算技术平台的独立性、完整性和安全性。从技术产品化落地由易到难的次序，隐私计算平台互联互通可分为以下三个层次：



◆ 未来隐私计算技术发展生态将更为开放，基于不同厂商的隐私计算平台对接的商业化、政务、企业等多种数据来源，将逐步构建数据与智能的计算网络，并通过预测模型、决策分析、客户画像等工具，进一步加速隐私计算落地于金融、政务、医疗等各类应用场景，构建一个由数据提供方、数据应用方、技术服务和运营方共同组成的全局数据智能网络生态。

- 1

简化了技术对接流程，当数据、模型、场景得以跨平台共享后，更便于共同构建隐私计算生态网络，并且可支持平台越多，越容易扩展生态网络
- 2

缩减了沟通与技术对接成本，对于有指定隐私平台的数据合作方可在不要求其必须本地部署行内平台的前提下快速落地业务场景，极大简化了业务流程
- 3

为数据安全治理提供补充思路，各家隐私计算平台应用机构使用同一套互联互通标准有助于监管部门统一管理，提升隐私计算发展的规范性和安全性

◆ 团队介绍：

亿欧智库（EqualOcean Intelligence）是亿欧EqualOcean旗下的研究与咨询机构。为全球企业和政府决策者提供行业研究、投资分析和创新咨询服务。亿欧智库对前沿领域保持着敏锐的洞察，具有独创的方法论和模型，服务能力和质量获得客户的广泛认可。

亿欧智库长期深耕科技、消费、大健康、汽车、产业互联网、金融、传媒、房产新居住等领域，旗下近100名分析师均毕业于名校，绝大多数具有丰富的从业经验；亿欧智库是中国极少数能同时生产中英文深度分析和专业报告的机构，分析师的研究成果和洞察经常被全球顶级媒体采访和引用。

以专业为本，借助亿欧网和亿欧国际网站的传播优势，亿欧智库的研究成果在影响力上往往数倍于同行。同时，亿欧EqualOcean内部拥有一个由数万名科技和产业高端专家构成的资源库，使亿欧智库的研究和咨询有强大支撑，更具洞察性和落地性。

◆ 报告作者：



宋世婕

亿欧智库分析师
Email: songshijie@iyiou.com



孙齐远

亿欧智库分析师
Email: sunqiyuan@iyiou.com

◆ 报告审核：



孙毅颂

亿欧智库研究总监
Email: sunyisong@iyiou.com

◆ 版权声明：

本报告所采用的数据均来自合规渠道，分析逻辑基于智库的专业理解，清晰准确地反映了作者的研究观点。本报告仅在相关法律许可的情况下发放，并仅为提供信息而发放，概不构成任何广告。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议。本报告的信息来源于已公开的资料，亿欧智库对该等信息的准确性、完整性或可靠性作尽可能的追求但不作任何保证。本报告所载的资料、意见及推测仅反映亿欧智库于发布本报告当日之前的判断，在不同时期，亿欧智库可发出与本报告所载资料、意见及推测不一致的报告。亿欧智库不保证本报告所含信息保持在最新状态。同时，亿欧智库对本报告所含信息可在不发出通知的情形下做出修改，读者可自行关注相应的更新或修改。

本报告版权归属于亿欧智库，欢迎因研究需要引用本报告内容，引用时需注明出处为“亿欧智库”。对于未注明来源的引用、盗用、篡改以及其他侵犯亿欧智库著作权的商业行为，亿欧智库将保留追究其法律责任的权利。

◆ 关于亿欧：

亿欧EqualOcean是一家专注科技+产业+投资的信息平台和智库；成立于2014年2月，总部位于北京，在上海、深圳、南京、纽约有分公司。亿欧EqualOcean立足中国、影响全球，用户/客户覆盖超过50个国家或地区。

亿欧EqualOcean旗下的产品和服务包括：信息平台亿欧网（iyiou.com）、亿欧国际站（EqualOcean.com），研究和咨询服务亿欧智库（EqualOcean Intelligence），产业和投融资数据产品亿欧数据（EqualOcean Data）；行业垂直子公司亿欧大健康（EqualOcean Healthcare）和亿欧汽车（EqualOcean Auto）等。

◆ 基于自身的研究和咨询能力，同时借助亿欧网和亿欧国际网站的传播优势；亿欧EqualOcean为创业公司、大型企业、政府机构、机构投资者等客户类型提供有针对性的服务。

◆ 创业公司

亿欧EqualOcean旗下的亿欧网和亿欧国际站是创业创新领域的知名信息平台，是各类VC机构、产业基金、创业者和政府产业部门重点关注的平台。创业公司被亿欧网和亿欧国际站报道后，能获得巨大的品牌曝光，有利于降低融资过程中的解释成本；同时，对于吸引上下游合作伙伴及招募人才有积极作用。对于优质的创业公司，还可以作为案例纳入亿欧智库的相关报告，树立权威的行业地位。

◆ 大型企业

凭借对科技+产业+投资的深刻理解，亿欧EqualOcean除了为一些大型企业提供品牌服务外，更多地基于自身的研究能力和第三方视角，为大型企业提供行业研究、用户研究、投资分析和创新咨询等服务。同时，亿欧EqualOcean有实时更新的产业数据库和广泛的链接能力，能为大型企业进行产品落地和布局生态提供支持。

◆ 政府机构

针对政府类客户，亿欧EqualOcean提供四类服务：一是针对政府重点关注的领域提供产业情报，梳理特定产业在国内外的动态和前沿趋势，为相关政府领导提供智库外脑。二是根据政府的要求，组织相关产业的代表性企业和政府机构沟通交流，探讨合作机会；三是针对政府机构和旗下的产业园区，提供有针对性的产业培训，提升行业认知、提高招商和服务域内企业的水平；四是辅助政府机构做产业规划。

◆ 机构投资者

亿欧EqualOcean除了有强大的分析师团队外，另外有一个超过15000名专家的资源库；能为机构投资者提供专家咨询、和标的调研服务，减少投资过程中的信息不对称，做出正确的投资决策。

◆ 欢迎合作需求方联系我们，一起携手进步；电话 010-57293241，邮箱 hezuo@iyiou.com



 亿欧智库

网址: <https://www.iyiou.com/research>

邮箱: hezuo@iyiou.com

电话: 010-57293241

地址: 北京市朝阳区霞光里9号中电发展大厦A座10层