隐私计算又被形象地称为“可用不可见”的技术，是涵盖众多学科的交叉融合技术，目前主流的隐私计算技术主要分为三大类：以多方安全计算为代表的基于密码学的隐私计算技术，以联邦学习为代表的人工智能与隐私保护技术融合衍生的技术，以可信执行环境为代表的基于可信硬件的隐私计算技术。

4月4日，北京国家金融科技认证中心公布了首批“多方安全计算金融科技产品国推认证”名单，包括蚂蚁集团两项产品在内的首批5项产品通过了该认证。

这是国内首次对多方安全计算金融领域应用展开认证工作，也是目前国内唯一针对该领域的“认证”，此次认证结果的发布，意味着数据要素市场的相关市场准入标准和监管体系迎来进一步完善。

作为隐私计算产品的重要底层技术，多方安全计算技术能够在保护数据隐私的同时，实现不同机构之间数据的合法合规融合，实现安全的多方数据查询和分析，进一步打破各方之间的数据壁垒，连接数据孤岛，有效实现数据价值的转化与释放。

为数据价值而生的隐私计算

伴随着云计算、大数据、人工智能等新一代信息技术的快速发展，数据已经成为基础性关键战略资源，同时也是数字经济时代的核心生产要素。

但是，在信息技术蓬勃发展的同时，数据也面临着一系列严峻的安全挑战，不仅包括公民个人信息和隐私的安全隐患，也包括政府和企业数据资产的泄露风险。近年来，数据泄露事件层出不穷，出于安全顾虑，数据价值链不同环节之间的流动受阻，分工协作关系脆弱，很难形成有效闭环。

大数据时代，如何在保障数据安全的同时又不影响数据要素的使用，是每一个数据生产者和获益者应该考虑的事情。

1982年，著名计算机学家、中国科学院院士姚期智提出了经典的“百万富翁”问题：张三和李四都是富翁，他们想知道谁更富有，但他们都想保护好自己的隐私，不愿意让对方或者任何第三方知道自己真正拥有多少财富。如何在保护好双方隐私的情况下，计算出谁更有钱？

在普通人看来，这几乎是一个无解的悖论。但是姚期智就此提出了“多方安全计算”的概念，即“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”。

近年来，我国多部与数据安全相关的法律法规落地实施，包括《网络安全法》《个

人信息保护法》《密码法》《数据安全法》以及《民法典》，形成了较为完备的安全法律体系，隐私计算为需求强烈但瓶颈重重的数据流通提供了破局思路。

随着政策落地以及各方关注度的提升，隐私计算已成为当下火热的新兴技术，跻身商业和资本竞争的热门赛道，有业界人士将2020年称为“隐私计算元年”。顾问咨询公司高德纳（Gartner）发布的《2021年重要科技战略趋势》中，也将隐私计算列为未来几年科技发展的九大趋势之一。

多技术融合保护数据安全

隐私计算又被形象地称为“可用不可见”的技术。看不见数据，却又能实现对数据的计算分析，隐私计算是如何做到的？

蚂蚁集团隐私智能计算技术部总经理王磊告诉科技日报记者，隐私计算是涵盖众多学科的交叉融合技术，发展初期汇聚了多种不同种类的技术，目前主流的隐私计算技术主要分为三大类。

第一类是以多方安全计算为代表的基于密码学的隐私计算技术；第二类是以联邦学习为代表的人工智能与隐私保护技术融合衍生的技术；第三类是以可信执行环境为代表的基于可信硬件的隐私计算技术。

以多方安全计算为例，其主要逻辑是在没有可靠的第三方（中介）的情况下，各方通过事先约定的密码学协议进行交互，完成预定的计算任务，每个参与方无法得知其他方输入的信息，只能得到计算结果。

“每一类技术路线都有各自的特点，适用于不同的应用场景。”王磊说，例如联邦学习适用于对性能和规模要求较高的建模场景，多方安全计算安全性更高，基于可信硬件的隐私计算可以支持更复杂的计算需求。

但是，从近年来的技术发展趋势和行业需求来看，想要通过单一技术“包打天下”几乎不可能，现实需求往往需要不同的隐私计算技术组合使用，在保证原始数据安全和隐私性的同时，完成对数据的计算和分析任务。

王磊告诉记者，以蚂蚁集团隐私计算的技术路线为例，从最早基于矩阵掩码的数据变换方案，到基于多方安全计算和可信执行环境的两套技术路线，再到后来的多种技术融合路线，并催生了可信隐私计算开源框架“隐语”和隐语开放平台。“隐语”提供的是代码，主要面向开发者，好比把原材料都准备齐全，就看开发者怎么做出一桌色香味俱全的大菜；而隐语开放平台则可以让用户直接调用各项功能，好比平台提供了预制菜，只要根据个人需求简单加热调味即可。

金融领域应用最广泛

当前，隐私计算应用最广泛的是金融行业。例如，招商银行启动了“慧点隐私计算平台互联互通项目”，交通银行则启动了监管沙盒项目，中国工商银行、中国农业银行也不同程度的在相关业务中尝试性地应用了隐私计算工具。

“传统的金融机构风险管理模式，除了调查走访外，主要是利用本单位数据和征信系统查询用户信息，这种方式对用户的风险判断不够全面。”王磊表示，基于多方安全计算的金融风控全链路解决方案，可以调用不同机构的多个信息渠道对潜在用户的历史记录进行多维度计算分析，各金融机构、信息渠道可形成征信系统联盟，能为各方提供数据分析服务，且数据无须离开本地，调用数据的过程中，数据不再以明文（即数据不加密）形式出现，而是通过安全协议共享，任何人都无法从中窥探到原始信息，这就是隐私计算相较于传统金融机构风险管理模式所带来的重要改变。

除了金融行业，隐私计算在医疗行业、保险理赔、政务信息等领域也有非常大的应用空间。

例如，过去保险机构在理赔过程中，会向医疗机构明文查询被保险人的诊疗情况，而获得的原始数据往往涉及用户隐私。2018年，蚂蚁集团尝试将隐私计算技术应用到保险理赔场景，通过设定数据逻辑查询，利用多方安全计算等隐私计算技术，使得保险公司只获得是否理赔的结果，不会获得原始数据，从而实现数据“可用不可见”，保护理赔用户隐私。

在医疗行业，全球抗击新冠疫情数据共享也运用到了隐私计算，这使各方可以在不公布详细数据的情况下，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，实现了对病毒流行病学情况的实时追踪和对未来毒株演化的预测，成为抗击疫情的一把利剑。

王磊表示，自计算机诞生以来，数据一直是明文流通和应用，面向数字经济时代，安全地用好数据成为绕不过去的坎。今后，法规政策和技术进步都将助推数据要素告别明文流通，开启“数据密态时代”的新征程，在数据密态时代最有潜力的支撑性技术非隐私计算莫属。

作者：张晔

来源： 科技日报