隐私计算联盟
Privacy Preserving Computing Alliance

可信隐私计算研究报告

（2022 年）

隐私计算联盟

2022 年 7 月

编写委员会

❖ **主要编写单位**（排名不分先后）:

隐私计算联盟、中国信息通信研究院云计算与大数据研究所、蚂蚁科技集团股份有限公司、上海富数科技有限公司、杭州趣链科技有限公司、深圳市洞见智慧科技有限公司、京东科技信息技术有限公司、深圳市腾讯计算机系统有限公司、同盾科技有限公司、上海浦东发展银行股份有限公司、北京数牍科技有限公司、深圳前海微众银行股份有限公司、深圳致星科技有限公司（星云 Clustar）、优刻得科技股份有限公司、杭州锘崴信息科技有限公司、中国工商银行股份有限公司软件开发中心、中国移动通信有限公司研究院、北京百度网讯科技有限公司、北京冲量在线科技有限公司

❖ **编写组主要成员**（排名不分先后）:

白玉真	袁　博	闫　树	王思源
魏　凯	姜春宇	刘嘉夕	贾　轩
杨靖世	童锦瑞	吕艾临	马智华
韦　韬	彭　晋	潘无穷	昌文婷
袁鹏程	卞　阳	杨天雅	徐　静
汪小益	韩梦薇	曾钰涵	王湾湾
杨　博	孙中伟	赵国梁	李克鹏
程　勇	贾金龙	陈　涛	郭林海
高　扬	金银玉	单进勇	范力欣
黄安埠	蔡烁玮	苗天麒	何永德
刘　沛	唐丹叶	李　帜	周建平
黄司辉	于　路	信　伦	于　欢
周吉文	陈浩栋	张亚申	

前言

隐私计算是在保护数据安全及个人隐私的前提下，实现数据流通及数据价值深度挖掘的一系列方法。近年来，数据成为国家基础性战略资源，在政策和市场的共同作用下，隐私计算技术、产业、应用迅速发展，已经从概念验证阶段开始逐步走向规模应用阶段。但是，在技术应用过程中，隐私计算因为涉及需求方、供给方、监管方等多方的参与，仍然面临着安全性、合规性、可用性等方面的挑战，由此隐私计算技术如何“可信”应用引发业界思考。

经过广泛调研征集和深入讨论，隐私计算联盟联合中国信息通信研究院云计算与大数据研究所等单位共同完成了《可信隐私计算研究报告（2022 年）》。本报告首先在隐私计算快速发展、相关技术融合创新、隐私计算理论不断演进的形势下提出了广义的隐私计算。然后，基于隐私计算应用过程中面临的挑战，从供给侧角度，梳理了技术可信应用的原则，首次明确提出并重点探讨了“可信隐私计算”的概念和五大核心要素。在此基础上，进一步分析了企业、行业的可信实践路径，提出了未来发展的相关建议。本报告致力于在隐私计算技术原理和应用实践之间搭建起连接的桥梁，为供给侧的企业产品研发和技术应用提供指导，推动隐私计算行业健康发展，让隐私计算在数据要素市场建设和数据流通过程中发挥更大的价值！

目录

第一章

可信隐私计算发展背景

（一） 隐私计算快速发展

隐私计算（Privacy-preserving computation）是指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，保障数据在流通与融合过程中的“可用不可见”[1]。在数据成为国家基础性战略资源的当下，隐私计算已成为需求强烈的数据流通“技术解”之一。Gartner 发布的 2022 年十二大重要战略技术趋势中指出，预计到 2025 年，60%的大型企业机构将使用一种或多种隐私计算技术（其称为“隐私增强计算”）。随着各方的积极布局，技术可用性的快速提升促使隐私计算市场由观望转向落地，隐私计算在各行各业多种应用场景中逐渐崭露头角。

1. 数据流通需求

发展数字经济是国家的重要战略部署，其中数据作为关键的生产要素之一，通过跨地域、跨行业、跨领域、跨机构的数据流通释放要素价值。但是，目前机构间的数据流通存在诸多阻碍。

数据流通面临产权制度未建立、安全共享存在风险、监管要求待完善等问题。一是数据的各种产权，如数据资源持有权、数据加工使用权、数据产品经营权等产权运行机制有待建立，为数据要素权益提供保护制度。二是数据流通存在安全风险。近年来，由于流通过程中

的数据安全事件时有发生，降低了企业参与数据流通的积极性。三是流通过程中的安全合规尺度难把握。现对数据可流通的对象、范围、方式等一系列落地问题，数据合规流通的细化规定尚未建立和完善。在此背景下，因缺乏统一、明确的合规监管体系和可行的技术实现路径，监管部门及数据使用者对数据流通中的安全合规评价尺度难以把控，导致很多数据流通需求仍处于理论探索阶段，难以实现。

“可用不可见”的隐私计算成为了上述问题的技术突破口。从原理上讲，隐私计算是一套融合了密码学、安全硬件、数据科学、人工智能、计算机工程等众多领域的跨学科技术体系，包含了以多方安全计算、联邦学习和可信执行环境为代表的多种技术方案。从应用目的来看，一方面，隐私计算通过对原始数据加密、去标识化或假名化处理，计算过程及结果只传递经处理后的数据，实现了原始数据不出域，保证了原始数据持有权不变且不受损，仅让渡了数据使用权，实现了数据的持有权和使用权相互分离，保障了数据主体的合法权益。另一方面，隐私计算通过限定数据用法、用量，解决了原始数据无限复制、盗用、滥用的问题。同时，隐私计算利用加密、去标识化或假名化处理后的数据进行计算，计算过程中只传递切片、密文等非原始数据，有助于实现对原始数据的最小化使用。另外，结合特定应用场景，经隐私计算技术去标识化处理后的数据在一定条件下有望实现匿名化，从而为多源数据的安全融合应用和价值释放提供了新思路。

2. 法律政策环境

当前国内多个法律和政策助推隐私计算产业进一步发展。

法律层面，一系列与数据及其安全保护相关的法律法规陆续发布，《国家安全法》《网络安全法》《数据安全法》及《个人信息保护法》等共同构筑了数据安全保护的基础性“法律堡垒”。

政策层面，2016年工业和信息化部、中国人民银行、国家发改委、中央网信办、国家能源局等各部委先后在相关政策文件中提出加强隐私计算相关技术的攻关和应用。2021 年 5 月，人民银行组织金融机构开展包括应用隐私计算进行数据共享在内的金融数据综合应用试点。2022 年 1 月，国务院办公厅印发的《要素市场化配置综合改革试点总体方案》中提出探索“原始数据不出域、数据可用不可见”的交易范式，探索建立数据用途和用量控制制度，实现数据使用“可控可计量”。4 月，《中共中央 国务院关于加快建设全国统一大市场的意见》明确提出，“加快培育数据要素市场，建立健全数据安全、权利保护、跨境传输管理、交易流通、开放共享、安全认证等基础制度和标准规范，深入开展数据资源调查，推动数据资源开发利用。”地方层面，目前已有十八个省市公布了相关数据条例，促进数据流通和开发利用[2]。

在技术优势和政策环境的助力下，隐私计算在不获取其他参与方原始数据的情况下处理数据，结合授权和防篡改等手段有效控制数据滥用，成为目前数据流通领域最受关注的技术热点之一。相关的学术会议和论文数量在近几年呈现大幅增长，研究也从技术原理逐步转向应用实践。在算法协议优化、软硬件结合方案提升计算性能之下，越来越多的企业入局隐私计算研发和产品化，产品逐渐开启商业化大规

模应用，在金融、医疗、政务、互联网、车联网等数据流通需求强烈的场景纷纷落地。

（二） 隐私计算技术理念外延扩展

国际方面，与隐私计算相关的概念有隐私增强技术（Privacy Enhancing Technologies，PETs）和隐私保护计算（Privacy-Preserving Computation）。其中隐私增强技术范围比较宽泛，把从系统层面实施数据保护协议的技术都囊括其中，而隐私保护计算则聚焦在具体技术[3][4][5]。例如，在欧盟网络安全局（ENISA）的定义中，除了隐私保护计算，隐私增强技术还可包括匿名化、假名化以及访问、通信、存储过程中各种实现隐私保护的技术。而联合国大数据工作组发布的技术手册中则将两种概念合并使用[6]。

国内方面，中科院信工所的李凤华等人[7][8]定义隐私计算（Privacy Computing）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、隐私泄露代价、隐私保护与隐私分析复杂性的可计算模型与公理化系统”。隐私计算联盟、中国信通院云大所在数据流通场景中对隐私计算概念进行延伸，《隐私计算白皮书（2021）》中定义隐私计算（Privacy-preserving computation）是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，保障数据在流通与融合过程中的“可用不可见”[1]。该定义被产业界广泛关注引用，更关注的是“保护隐私的技术或方案”。

而今，各界对隐私保护的需求越来越重视，隐私计算概念也有了

新的概念外延。例如今年 5 月，美国《促进数字隐私技术法案》[9]将隐私增强技术明确为“通过提高可预测性、可管理性、可分离性和保密性来减轻数据处理所产生的个人隐私风险的任何软件或硬件的解决方案、技术流程或其他技术手段。包括:（1） 促进数据计算或分析，同时减轻隐私风险的加密技术;（2）公开分享数据但不对特定个人作出推断的技术;（3）让个人控制其数据的传播、共享和使用的技术;（4）产生合成数据的技术”。

因此，本报告与时俱进，从隐私计算实现的目标，将隐私计算技术[1]进行扩展，促进实现隐私保护和共享数据价值分析的技术方案均可纳入隐私计算的范畴。

广义隐私计算是面向隐私信息全生命周期保护的计算理论和方法，涵盖信息所有者、信息转发者、信息接收者在信息采集、存储、处理、发布（含交换）、销毁等全生命周期过程的所有计算操作，是实现隐私保护前提下数据安全共享的一系列技术。技术体系如**图 1** 所示，包括但不限于:

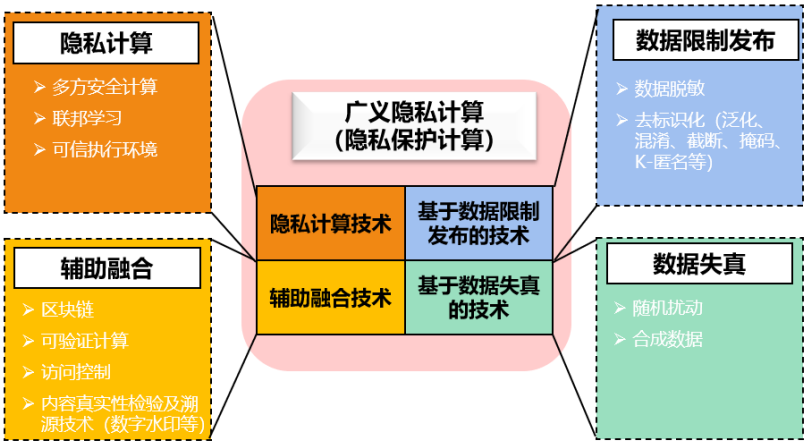

图 1 广义隐私计算技术体系

1. 隐私计算技术

隐私计算技术，以多方安全计算、联邦学习、可信执行环境三大路线为基础，还包括同态加密、零知识证明等辅助技术。这些技术分离了数据的持有权和使用权，实现多方数据在保护隐私的前提下联合计算，使数据需求方在不接触原始数据的情况下获得数据的增值价值，降低隐私泄露风险。

2. 基于数据限制发布的技术

基于数据限制发布的技术，有选择地发布原始数据、不发布或者发布精度较低的敏感数据从而实现隐私保护，包括数据脱敏以及各类去标识化技术（如掩码、抑制、泛化、截断、混淆、k-匿名、l-多样性、t-贴近等）。这类技术保证对敏感数据及隐私的披露风险在可容忍范围内，但是需要考虑数据隐私披露和可用性之间的平衡，隐私保护的强度越强，丢失的信息就越多，数据的可用性越低。

3. 基于数据失真的技术

基于数据失真的技术，通过添加噪音等方法，使敏感数据失真但同时保持某些数据或数据属性不变，仍然可以保持某些统计方面的性质，包括随机扰动、合成数据技术等。数据失真是一种能够抵御背景知识攻击的隐私保护方法，这类方法不依赖复杂的密码学技术，用户计算开销小，并可获得精准的查询结果。

4. 辅助融合技术

隐私计算最核心的是计算，但整个数据共享过程以及完整的系统需要借助多个辅助技术支撑，包括区块链、可验证计算、内容真实性

检验及溯源技术（如数字水印）和访问控制技术等。这些技术虽不是完全直接实现数据的联合隐私计算，但能在数据共享过程中有效保护个人信息，实现全流程可记录、可验证、可追溯、可审计、可控制的安全、可信的数据共享，为数据真实性、数据确权等问题提供可行解决方案。

（三） 隐私计算应用需建立信任原则

隐私计算正处于技术快速迭代和发展的阶段，为企业和机构当前面临的数据合规监管、数据安全制度落地提供有力的技术支撑。但是，企业应用技术的过程中，技术的安全性、合规性、性能、稳定性、可扩展性、互联互通等方面仍存在困难和挑战，在一定程度上限制了隐私计算的推广和应用。

1. 安全共识有待形成

隐私计算产品的安全性是技术应用中面临的首要问题。安全性不仅仅是算法协议安全，开发应用安全、安全性共识和安全性可验证也都是技术应用需要关注的核心问题。

算法协议尚无法实现绝对安全。一是算法协议多样，各自协议的安全根基各不相同：多方安全计算基于密码学，联邦学习基于分布式机器学习、差分隐私等，可信执行环境依赖于硬件。二是产品依赖安全假设（如硬件提供商可信赖、计算参与方完全遵循协议流程），但实际中安全假设不一定完全成立，可能存在安全风险。

开发应用安全存在挑战。一方面隐私计算产品面临生产化过程中的安全问题，如密码学算法领域的侧信道攻击，恶意黑客攻击。另一

方面通过引入第三方带来了不确定风险因素，如利用第三方生成乘法三元组或第三方分发密钥，可能会打破信任的完整性。

安全性标准亟需建立。隐私计算涉及的密码学原理复杂、应用场景多样化，隐私计算参与者很难通过直观的方法验证所用产品的安全性。因此，有待建立隐私计算产品的系统性安全分类分级标准和开发相关安全验证工具。

2. 合规适配仍要探索

隐私计算作为一种数据安全保护措施，通过原始数据最小化处理、去标识化等安全保障方式有助于提升数据流通的合规性，但是和法律的适配性仍要继续探索。一是，就匿名化而言，当存在反向推演出可复原识别特定信息主体的可能性时，数据的使用仍需参与方获得用户授权同意，而获取个人完全符合法律要求的授权同意难度极高。二是，联合建模过程中，隐私计算因交互传输梯度等衍生信息，存在泄露原始数据的可能性，如参与方对隐私计算活动怠于安全管理或安全管理不到位，将可能导致未尽安全管理义务等方面的合规风险。三是，部分参与方可能会恶意合谋获取其他参与方的数据，存在暴露或推导其他方数据的隐患，如参与方之间不遵守合约和诚信原则，将可能导致非法获取特定数据等方面的合规风险。四是输出计算结果时，如不积极采取包括技术、法律等多项防范措施予以防止，可能存在用户的隐私信息泄露风险，例如在金融机构和征信机构的联合风控场景中，若泄露了借款人的个人身份标识信息，则可能泄露借款人的借款需求。

3. 可用瓶颈亟需突破

性能、稳定性、可扩展、互联互通等可用性的需求强烈且要求高。一是密文计算消耗大量计算和通信负载，多方参与中最薄弱的一方或一环将成为计算瓶颈。二是多节点、大规模应用情况下，如金融、通信场景，需满足同步在线、同步计算、实时响应等要求。三是在隐私保护要求高、数据来源多、数据规模大分布广、业务线条复杂、交互频繁的场景中，为更好契合实际业务需求，对系统的稳定性、可靠性、扩展性、兼容性和场景支持能力等也提出了新的挑战。四是目前市场上的系统产品大多闭源，平台之间由于算法的复杂多样、技术方案的不同、应用生产环境组件的差异化难以互通，导致系统重复建设和增加用户部署、运营成本，互联互通壁垒或造就“数据群岛”。

4. 建立信任是必经之路

隐私计算实现数据价值的流通，最终受益的对象是人，根本应该是人信任技术。隐私计算的发展需要关注用户的需求、背景等各种因素，建立信任原则，随着社会对隐私计算信任的提升，隐私计算技术将得到更广泛的应用，发挥更大的价值。

各界高度关注隐私计算应用。技术层面，学术界对安全的算法协议、安全效率的平衡等难题展开研讨，并一直保持火热的研究态势。政策层面，隐私计算技术应用中的合规问题探讨持续进行。企业层面，联邦学习 FATE 开源社区提出了可信联邦学习[10]，蚂蚁集团提出了可信密态计算[11]，从概念理念上开始初步探索。行业层面，隐私计算联

盟（PPCA）、中国通信标准化协会大数据技术标准推进委员会（CCSA TC601）、全国信息安全标准化技术委员会（TC260）、北京金融科技产业联盟、IEEE、ITU 等多个标准化组织积极布局隐私计算安全性、性能标准，场景应用规范、合规指南等内容。

本报告通过梳理隐私计算技术应用中的主要原则，从供给侧企业研发产品的角度提出了“可信隐私计算框架”，作为隐私计算产品落地指导的一套方法论，从应用、产业等维度围绕企业和行业的可信实践进行深入剖析，致力于在隐私计算技术原理和应用实践之间搭建起连接的桥梁。

第二章

可信隐私计算框架

“可信”一词近年来主要出现在计算机领域的“可信计算”（Trusted Computing，TC）的概念中。可信计算主要强调的是计算机系统和其处理过程的可预测性、可验证性，保证全部计算过程的可测可控和不被干扰，从而保证计算结果与预期的一致性。与传统计算机领域不同，隐私计算是一个复杂的系统工程，包含技术、法律等多方面应用的考量，因此，隐私计算领域中可信的概念需要被重新诠释。

可信隐私计算在应用过程中，其安全性、可用性和隐私保护能力等应符合设计声明预期，以满足数据需求方、数据提供方和监管方等各方的需求，一般包含安全可证、隐私保护、流程可控、高效稳定、开放普适等基本特征。图 2 给出了可信隐私计算的总体框架。

图 2 可信隐私计算总体框架

支撑技术层面，围绕着安全可证、隐私保护、流程可控、高效稳

定、开放普适等可信的基本特征，以理论研究为抓手，弥补当前技术的不足，缩小应用的差距。例如研究能抵抗恶意攻击、合谋攻击的安全保护技术、研究保证精度损失可接受条件下性能有效提升的技术方法、研究保证计算全流程可审计的技术方法等，都需要学术界和工业界的积极探索。

企业实践层面，隐私计算从概念验证到应用落地依赖于企业将技术产品化。因此，企业在可信隐私计算的应用实践是可信方法中至关重要的环节。同时，应该注意到没有完美的技术，关键在于如何正确的使用技术，需要在产品研发使用的全生命周期过程中贯彻可信特征的要求，从产品源头保证“可信”。

行业组织层面，可信隐私计算需要整个行业的参与，包括可信隐私计算标准体系的建设、可信隐私计算评估测试等，通过可度量可验证的方式来减轻隐私计算技术和系统应用带来的风险。

第三章

可信隐私计算核心要素

随着社会各界对隐私计算信任问题的不断关注，可信隐私计算技术已成为研究领域的热点。研究的焦点主要围绕隐私计算系统的安全性、隐私保护能力、效率、稳定性、适用性、扩展兼容、场景易用等方面的特性展开，这些特性也构成了可信隐私计算的核心要素。

（一） 第一要素：安全可证

安全可证是可信隐私计算的第一要素。隐私计算通过只输出中间参数、标签等信息，或通过在可信受控环境中对数据进行处理的方式，保障了数据的安全性，提高了数据流通的主动性。但隐私计算的安全性自证是技术应用过程中面临的难题，隐私计算产品安全边界的界定需要考虑不同行业、不同场景和不同技术的差别，也需要平衡计算准确性和计算效率的要求。因此，如何评价和验证系统的安全性亟需明确。

1. 安全性评价维度

虽然隐私计算的核心是计算，但是从技术应用和产品的角度，除了算法协议原理的安全性，还需综合考虑算法工程化实现、产品使用的密码模块和通信框架、调度管理功能的设计与实现等多方面的安全性。评价维度主要包括以下四个方面，整体系统的安全性由其中最薄弱的环节来界定。

一、**算法协议安全直接划定了产品整体的安全基线**，通常在应用

中需根据具体的安全需求选择不同算法，实现安全和效率的平衡。算法安全的评价维度主要包括:算法逻辑安全、安全假设、不诚实门限、安全参数、数据保护程度以及算法实现安全等指标。

二、**密码安全是隐私计算安全的重要支撑**。产品中各个功能模块的保密性、完整性都需要密码技术支撑，密码安全的重要性毋庸置疑。密码安全的评价维度主要包括：密码算法安全强度、密码算法使用正确性、密钥管理安全等。

三、计算过程通常涉及大量的通信交互，为了防止交互过程泄露数据隐私，**通信安全也需要得到保障**。通信安全的评价维度主要包括:通信信道安全、通信数据的保密性与完整性、通信过程抗重放攻击、通信数据篡改响应等。

四、**平台工程安全是产品安全的关键基础**。借助有效的身份认证、访问控制等手段，保障平台服务的保密性、完整性；还应保证各项功能模块的实现安全性，不应存在已知的或已公布的高危安全漏洞。平台工程安全的评价维度主要包括：授权认证、系统安全（安全漏洞、端口开放等）、存储安全等。

最后，隐私计算系统安全性度量应该考虑攻击者需要付出多大的努力来攻破给定的安全防护保障，以及信息泄露产生的后果或影响。一方面，产品不存在绝对的安全，大部分商业应用场景中，绝对安全的代价之高是难以承受的；另一方面，隐私计算的安全性需要结合性能、成本等因素综合考虑以满足场景的需求。为达成该目标，可设置不同的安全等级来衡量、区分隐私计算的安全性强弱，**根据实际应用**

场景选择适合的安全等级。在安全基线的设置上，应覆盖从产品基本的系统安全（如不存在中高危安全漏洞）到交互协议中信息熵泄露的审计能力和控制能力等各层级的安全要求。对通用场景，可信隐私计算应满足各个安全性维度的基础安全要求，防止因某个脆弱点而导致数据隐私泄露问题；对各类安全假设、数据敏感性不同的应用场景，产品应选择适合其场景特性的安全等级作为安全基线，在满足该等级安全目标的前提下，尽可能地提升可用性。

2. 安全性可验证

可信隐私计算的安全性应是可验证、可度量的。验证隐私计算安全性的技术门槛较高，需要通过各类方法对安全原理、安全实现等方面进行审核验证。考虑到隐私计算的技术路线和产品比较丰富，安全性验证应采用一个相对通用的尺度，端到端的进行。

根据验证角色的不同，验证形式主要有以下三种:

一是权威机构验证，指定权威的第三方机构进行详细和尽可能全面的审核测试。例如中国信通院“可信隐私计算评测”通过产品资料审核、测试报告审核、质询与答疑、集中评议等环节对企业产品的安全性进行全面评测[12]。

二是对用户开放，授权用户进行审核验证，用户根据业务需求及相关标准对产品进行详尽的审核。该种验证形式要求用户对安全性原理及其实现有充分的理解和把握。

三是完全开放（开源），通过公开代码使得外界能够完全了解技术原理和实现，可以接受行业专家的攻击验证，一般具有一定活跃度

的开源项目的安全性更透明、安全风险更明确，安全性更容易得到保障。

验证内容主要包括：原理论证审查（如形式化证明、参考论文、专家审查报告等）、系统设计文档审查（如算法协议、数据交互流程图、安全设计说明等）、核心代码检查、抓包报文分析、日志审核、模拟动态攻防等。

验证结果需满足：原理（密码算法、协议等）已验证有理论依据；系统设计符合安全性要求，与安全性原理材料保持一致；日志、代码、报文显示与安全性原理材料、系统设计文档保持一致。除此之外，还可采用基于安全攻防的深度安全评估和代码形式化证明的方式进一步验证。

（二）核心要素：隐私保护

隐私计算的核心目标是要保护隐私。个人隐私信息如个人身份标识、属性行为、位置轨迹等一旦泄露、非法提供或滥用将会危害个人或组织的相关权益。可信隐私计算通过技术手段对数据隐私进行保护，并将进一步保障数据使用可控，有效防止了数据的盗用、滥用和误用。**可信隐私计算要对全周期隐私信息有保护。**数据在不同参与方实体之间流转时，应采用隐私计算等技术措施，增强个人对处理者的信任度，应履行采取相应的隐私保护技术措施的义务，防止未经授权的个人信息泄露、篡改和丢失。

隐私计算能够实现多个数据所有者在互不信任的情况下进行协同计算，输出计算结果，并保证任何一方均无法得到除应得的计算结

果之外的其他信息。实践中，可以通过区间化、泛化/有效位截断、k-匿名、l-多样性、t-接近、差分隐私等方法对个人身份标识信息、属性行为数据等进行去标识脱敏处理，结合密码学技术、可信硬件等可信受控环境将数据转化为密态数据，从而实现相对匿名化。

此外在计算过程中，保证原始数据隐私信息不泄露的前提下，应对信息熵的保护程度进行识别、度量和控制，满足不同场景、不同数据生命周期内对用户隐私信息保护的要求。例如在结果对外输出前，可以进行差分隐私、泛化等处理，从而降低从结果中泄漏隐私信息的风险。以差分隐私为例，在数据结果上增加可度量的噪声预算，用于控制结果中信息熵不超过一定的阈值，进而保护原始数据的隐私信息，也有助于实现全周期隐私信息最小可见。

（三）信任基础：流程可控

隐私计算虽有不同的技术路线，但是由于涉及多个参与方、普遍依赖密码学方法进行计算，所以数据使用的可控可计量、计算流程的可监控、全流程的可审计等至关重要，这些也是用户信赖隐私计算产品的基础。

1. 事前明确授权

为保证数据使用的合规性，应事先对涉及的个人信息、商业秘密等隐私信息进行去标识化、脱敏等处理，并保证已获得数据方授权。数据授权时应明确授权主体，授权条件、授权内容、数据使用范围，明确业务过程所应用的隐私计算技术类型以及全过程所涉及的个人信息处理方式。通过数据预处理、假名化、加密、去标识化、原始数

据与计算数据分离等方式，避免在后续的数据流通过程中产生模糊不清的地方。获取数据主体授权的服务平台可以通过区块链上的可信记录结合零知识证明等隐私计算技术对授权主体进行去中心化身份认证等措施保障授权行为的真实性验证和可回溯查证。

此外，可信隐私计算也应事先建立应急响应机制和相应的风险防范预案。一旦发现数据使用者有不合规的行为，数据持有方可以通过销毁授权凭证来撤销对数据使用者的授权，即使数据使用者留存了加密后的共享数据，也会因为无法解密而失去使用价值。

2. 事中过程可监控

隐私计算通过密态数据的计算来实现数据价值的流通，为满足隐私计算流程的有序合规，应保证计算过程可监控、数据使用可控可管。区块链技术和可信硬件相关技术常常被融合应用于数据流通管控机制中。例如首先通过区块链进行分布式多方可信的数据目录管理，利用可信执行环境、可信平台模块（TPM）和智能合约等保障数据用途、用法、用量的可控可管。其次基于区块链智能合约技术，通过白名单、合约终止、合约销毁、共识投票等方式对存在问题的合约进行处理，进一步提升隐私计算的可控性。

3. 事后可验证可审计

计算过程应满足可验证。计算过程既决定了数据是否按照设计的协议严格执行，也决定了计算结果是否正确。计算过程的可验证性结合可验证计算协议来实现。基于复杂性理论的交互式证明系统、概率可验证证明系统或密码学理论构造的可验证计算协议能够以较高的

正确率判断出计算过程是否正确。另外，类似可信执行环境等拥有硬件可信计算基的计算环境也能够对外部系统提供计算一致性度量，基于远程证明机制可以提供计算过程的可信验证能力。

除此之外，隐私计算全过程也应满足可审计可追溯。将隐私计算全过程中各参与方的操作行为、模型参数、状态信息、计算过程、数据的访问记录等信息进行存证，保证隐私计算的可审计性。与隐私计算结合的区块链技术拥有多方参与、数据全节点可见、链上数据可追溯、不可篡改的特点，因此常用于辅助存证审计。例如，参与方通过对用于模型训练和预测的运行代码和中间数据进行存证，确保整个训练和预测过程中的可复现性与不可抵赖性。参与方也可对数据流通过程中的关键安全事件进行记录，如对敏感事件（访问其它参与方的数据等）、关键事件（非授权或不合法的行为等）、出域的数据传输等事项进行存证，从而提升隐私计算的透明性与可信度，降低责任追溯的难度。

（四）落地抓手：高效稳定

除了具备安全可证、隐私保护、流程可控，想要实现隐私计算系统的真实可用和场景落地，高效稳定是可信隐私计算应用的重要抓手。

1. 性能可用

计算性能瓶颈亟需突破。首先，隐私计算的安全性、计算效率与计算精度之间存在一定程度上的矛盾。一是为了实现计算安全性，理论上来看隐私计算一定会付出比明文计算更大的计算和存储代价，目前与明文相比至少有 1-2 个数量级的差距。二是某些特定算法（如差

分隐私）虽然效率高但是会损失部分精度，导致计算结果与明文存在一定程度的偏差。其次，多个参与方之间的多轮信息交互，通信开销较大，部分应用场景中数据规模大、数据具有异构性且计算实时性要求高。

因此，可信隐私计算系统应在保证数据安全和精度可接受的前提下，尽量支持大规模、高并发计算以及满足业务场景的特定要求（如金融场景模型在线推理的实时性要求）。产品可以通过分布式并行计算、算法优化（如降低算法耦合度）、通信优化（如通过模型压缩减少通信量）以及软硬结合（如计算加速卡、专用密码计算设备、一体机）等多种方式来进一步提升性能。

2. 稳定可靠

系统可靠性是系统可用时间占总时间的比例，当大规模应用时，可信隐私计算系统的可靠性应满足场景需求，达到99%以上，甚至到99.999%。

一方面，系统应通过一系列技术手段来降低故障发生的概率。如通过灾备设计（主备、多活等）使得在单节点出现故障时可自动隔离及切换；在服务器、硬盘、网络、节点等出现故障后，可以进行自动容灾恢复，包括数据的备份和恢复、计算任务的恢复等。

另一方面，系统也要降低故障发生后的影响范围。分布式系统的各服务节点需要具备完善的日志、监控指标、链路追踪等可观测手段，准确观测系统（网络、内存等）运行情况，通过监控告警及时定位并处理问题，有效提升故障发生后的处理效率。

（五） 规模化前提：开放普适

日渐增加的隐私计算产品在丰富市场选择的同时也带来了新的需求，一是技术实现方法的多样化使得不同技术平台所托管的数据无法跨平台交互，可能造成“计算孤岛”现象，由此市场对平台的开放扩展兼容能力、互联互通能力提出了新的要求；二是系统操作简便、容易部署、容易运维也是实现各行业场景落地、规模化应用必不可少的前提条件。

1. 开放灵活

为了应对将来需求的变化，可信隐私计算系统要具备可扩展、可迁移、可兼容、互联互通等特性，从而降低用户使用成本。

开放性方面，隐私计算系统应具备可兼容的能力，如支持隐私计算主流技术、相关辅助技术等不同技术之间的融合，支持隐私计算系统与大数据 ETL 系统、数据仓库、机器学习算法库等用户系统的兼容性。同时，系统也需尽量具备跨平台产品互联互通的能力，具备用户二次开发的能力，从而降低隐私计算技术应用的门槛。

灵活性方面，隐私计算系统需具备可扩展的能力，如支持任意的参与方数量、支持组件热插拔、组件热升级等；具备可迁移的能力，如支持内部的计算、存储、通信、调度等多个模块之间根据不同业务场景的需求实现不同层次的解耦，进一步实现不同模块跨异构平台的模块化迁移使用。

2. 场景易用

可信隐私计算系统易用性主要包括：支持如数据管理、任务管理、

模型管理等交互操作界面和可视化拖拉拽操作，降低用户理解、学习和使用的成本；提供算法开发框架，方便用户二次自定义算法；能在物理机、云环境、虚拟机等多种环境部署，且支持容器化部署；具备完善的部署和操作说明文档，方便用户理解、部署、使用和运维。同时，还需要满足业务场景的特定要求，切实做到可用易用，实现普适隐私计算。

第四章

可信隐私计算实践路径

结合可信隐私计算的核心要素，本报告从企业、行业两个层面总结提出了可信隐私计算的实践路径。企业层面，需要将可信隐私计算的要求嵌入到产品设计、研发、测试、运营使用的全流程中；行业层面，需要构建可信隐私计算标准体系、开展评估验证，从而推动隐私计算技术规范应用，完善整个产业生态。

（一）企业层面，将可信要素嵌入系统研发应用全流程

1. 规划设计阶段

企业在隐私计算系统生命周期的开始就需要充分考虑落实可信隐私计算的核心原则，将可信的理念根植于需求分析和系统详细设计等规划设计的关键环节中，从而使后续的研发过程能够始终符合可信的核心要求。

2. 研发测试阶段

安全可靠方面，着力提升隐私计算系统自身的安全能力。例如，提高算法协议抵抗恶意攻击、合谋风险的能力，提高对恶意攻击检测和追溯的能力；发生安全性问题时，应具备应急处理机制或直接终止计算任务的能力。隐私保护方面，积极采取相关技术措施，防止未经授权的个人隐私信息的泄露、篡改和丢失；开展信息熵识别、度量和

控制的相关技术研究，对不同计算场景下泄露的信息熵进行严格控制。流程可控方面，保证计算过程的可监控、计算全流程的可审计、提升系统的问题可追溯能力，确保系统及服务的可信性。高效稳定方面，基于理论研究、工程实现持续重点提高计算性能，以满足更多业务场景的需求。开放普适方面，加强企业间合作、加快互联互通规范落地，持续提升产品易用性，从而推动行业场景规模落地。

3. 运营使用阶段

在隐私计算系统落地运营使用阶段，需要做好运维及后续保障工作，需要持续监测隐私计算系统的各项可信风险，持续优化隐私计算系统。

（二）行业层面，打造可信隐私计算产业生态

可信隐私计算的实现不仅仅是企业的实践就足够，更需要多方参与协同，最终形成一个相互影响、相互支持、相互依赖的良性生态。

首先，标准化组织积极构建可信隐私计算的标准体系。政策法律只能规定原则和底线，需要标准从可执行可落地的层面进行具体指导和约束。目前，CCSA TC601、TC260、IEEE、ITU 等多个标准化组织已经发布或正在编制多个隐私计算产品或应用场景的相关标准规范。例如，今年 6 月《人工智能 隐私保护机器学习系统技术要求》和《人工智能 可信联邦学习技术规范》国家标准召开标准草案编制会，中国信通院联合隐私计算联盟编制金融场景应用规范《隐私计算 面向金融场景的应用规范》。

其次，权威机构积极开展企业产品的评测验证。权威机构评测是

检验目标对象是否达到相关要求的有效手段，由于隐私计算技术的复杂性，更加需要专业的第三方机构给予全力支持。围绕可信隐私计算的核心特征，要重点考虑隐私计算系统的安全性、隐私保护能力、流程可审计性、性能、稳定性和场景应用等方面的表现。中国信通院云大所、隐私计算联盟自从 2019 年至今，已经进行 6 个批次的“可信隐私计算评测”，涉及 102 家企业、124 个产品的评测[13]，已经成为供给侧产品研发和需求侧采购选型的风向标。

第五章

可信隐私计算发展建议

打造可信赖的隐私计算系统已经成为各界关注的焦点和努力的方向。通过实践可信隐私计算方法论，有助于提升隐私计算的可信水平，让其更好的被社会大众接受。可信隐私计算并非一成不变，而是伴随着法律法规的完善、隐私计算技术的发展，将会不断演进以适应新的发展需要，因此，各方需要从更加务实的角度出发，积极协作共建可信隐私计算体系。

（一） 政府层面，推进我国隐私计算监管进程

积极推进隐私计算监管细节落地和监管工具研发。目前尚无相关政府指南文件与产业工程实践具体结合，在数据流通的迫切需求下，亟需推进制定数据合规流通的细则文件，从而细化隐私计算产品的监管要求。与此同时，隐私计算企业如雨后春笋般涌现，纷纷入局研发产品，但是产品的可监管性仍有待提升，可以通过研发智能化监管工具，提高监管效率和灵活性。

（二） 技术层面，全面进行技术前瞻性攻关研究

开展可信隐私计算一体化研究，将是未来重点趋势。当前针对可信隐私计算的研究多是从安全性、可用性、易用性等维度开展的单一研究。已有工作表明安全性、效率、精度等不同要求之间存在相互制约的关系，若只考虑单一的要求会造成其他要求的冲突。因此，需要

针对可信隐私计算构建一体化研究框架，实现不同要素的最优动态平衡。

积极探索促进数据流通的技术，进行前瞻性布局。目前隐私计算系统主要基于多方安全计算、联邦学习和可信执行环境三大方法进行设计研发，随着隐私计算理念的不断扩展，学术界、企业需要积极探索广义隐私计算技术以及更多满足隐私保护需求下、促进数据流通的技术，从而研发相关数据流通产品、搭建数据流通基础设施。

（三） 企业层面，加快业务场景可信应用

加快可信隐私计算的落地应用，为业务赋能。一是，数据密集型场景先落地，起到示范带头的作用，例如在金融、政务、互联网、医疗等场景创建先行示范应用。二是，企业应当探索隐私计算各分支技术间、隐私计算与外部技术间的融合方案，为数据可信流通及拓展应用边界夯实技术基础，为业务的发展赋能。三是，积极推动隐私计算产品互联互通的可行方案和落地实践，有效降低应用成本。

（四） 行业层面，积极开展评测推动规范应用

积极开展可信隐私计算评测，推动可信隐私计算产业生态。可信隐私计算是一项复杂的系统化工程，需要多方共同参与。应充分发挥行业组织优势，搭建合作交流平台，广泛吸纳行业优秀的实践经验，完善可信隐私计算标准体系，促进行业共识。围绕可信要素，加快研发自动化评测工具，全方面多角度地开展评估测试，持续规范可信隐私计算技术应用落地。

参考文献

[1].中国信息通信研究院云计算与大数据研究所. 隐私计算白皮书（2021）[R], 2021

[2].深圳数据经济研究. “18 省市公布『数据条例』” https://side.cuhk.edu.cn/article/349

[3].European Union Agency for Network and Information Security. Readiness analysis for the adoption and evolution of privacy enhancing technologies[R], 2015

[4].Kaitlin Asrow and Spiro Samonas. Privacy Enhancing Technologies: Categories, Use Cases, and Considerations. Federal Reserve Bank of San Francisco[R],2021

[5].CB Insights 中国. 中国隐私计算技术与市场发展研究报告[R], 2022

[6].Privacy Preserving Techniques Task Team. UN handbook on privacy-preserving computation techniques[R], 2019.

[7].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(4), 1-11.

[8].Fenghua Li, Hui Li, Ben Niu, Jinjun Chen. Privacy Computing: Concept, Computing Framework, and Future Development Trends[J]. Engineering, 2019,(05),1179-1192

[9].The House Committee on Science, Space, and Technology. H.R. 847, Promoting Digital Privacy Technologies Act[R],2022, https://www.

cbo.gov/publication/57941

[10]. 凤凰网. “杨强院士：希望 2022 年实现从联邦学习到可信联邦学习的跨越”,2022, https://tech.ifeng.com/c/8Edjy4R0IRe

[11]. 韦韬,潘无穷,李婷婷,等. 可信隐私计算：破解数据密态时代“技术困局”[J]. 信息通信技术与政策, 2022,48(5):15-24

[12]. 隐私计算联盟. “中国信通院公布第六批可信隐私计算评测结果”, 2022, https://mp.weixin.qq.com/s/0Jv0nhBedWXFSBceRstxdw

[13]. 隐私计算联盟. 隐私计算应用研究报告（2022 年）[R], 2022

联系方式：

中国信息通信研究院 云计算与大数据研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

邮箱：baiyuzhen@caict.ac.cn

网址：www.caict.ac.cn