CCF-之江实验室“智海计划”联合创新基金
课题申报指南

（一）知识驱动的人工智能

1.面向多模态信息网络的知识表达与计算

研究内容：多模态信息网络的知识表达与计算对于实现强人工智能具有重要意义，本指南旨在突破当前主要由数据驱动的多模态表示学习与融合技术，依据“数据-信息-知识-智能”的进化机制，以智能为目标。研究基于数据和信息的知识抽取与提炼技术；研究跨模态与跨领域的知识对齐融合与统一表达范式；研究动态交互式知识自组织演化理论与计算方法；建立多模态信息网络智能化知识表达与计算体系，打造数据-信息-知识-智能一站式计算框架与平台。

主要指标：（1）在至少千万级信息网络中，实现 3 种及以上模态数据特征自动化提取、表征和融合，算法能应用到实际应用场景中；（2）从超大规模信息网络结构与多模态信息内容中萃取关键知识并形成知识库，实现数据-知识双驱动下的智能化应用，性能超越现有单数据或者单知识驱动系统；（3）发表人工智能/数据挖掘领域 A 类会议 2-3 篇。

2.因果知识通用表达和效应估计方法研究

研究内容：（1）面向复杂决策场景，通过融合人类通用及领域知识和观测数据，设计和实现一种通用因果知识表达方法，支持在高维和多类型数据业务场景（可涉及医疗、教育、金融）中自动和高效的生成因果知识表达。（2） 基于通用算法生成的因果知识表达，设计

一种在部分变量不可观测条件下估计变量对之间的因果效应值和置信区间的方法。

主要指标：（1）构建示范案例，需覆盖医疗、教育和金融的 1-2 个场景；（2）因果知识表达形式中涉及连续和分类 2 种类型变量；（3）因果效应估计方法满足高效处理枚举状态数 200 及以上的变量或者变量集合；（4）发表或录用高水平论文 2 篇，申请国内发明专利 2 项。

3.图形表格知识抽取与图谱构建研究

研究内容：人类的科学技术知识大量沉淀在科学出版物，教科书，互联网文章，商业报告等文档中。而表格，图形，设计图，示意图等等更是其中重要的知识表达形式。传统的光学字符识别（OCR）技术无法对这类信息源做理解，更不能在此基础上构建完整的知识图谱。本指南旨在研究一种以机器视觉理解为基础的算法和系统设计，使得机器可以理解出版物的表格，图形，设计图，示意图等等的内生知识，并将其表达为机器可识别和推理的知识图谱。

主要指标：（1）构建并交付十万量级及以上的图形表格知识抽取训练及评测集，并提出对知识抽取精度的合理评测方案；（2）提出的知识抽取技术可应用于 2 种不同的表格或图形形态，其精度可以对标类似 DVQA 的 85%左右的问答准确性，并交付相应可复现代码；（3）在知识抽取的基础上，可对科学文档完成跨多图形，表格以及自然语言文本构建知识图谱（中文语言）；（4）发表或录用高水平论文 2 篇，申请国内发明专利 2 项。

4.多模态时序知识图谱建模与抽取技术研究

研究内容：大多数知识图谱基于非实时静态数据构建，智慧教育、智能制造等领域知识的时间与时序特性研究较少。目前，时序知识图谱研究处于起步阶段，基于深度学习模型抽取时序关系的准确率在80%左右，难以满足实际应用需求。本指南旨在研究一种多模态时序知识图谱的建模与抽取方法，使机器可以从书本、教学课件、标准化文件等多模态数据中理解学习知识点、科学方法，生产工艺流程步骤等的前后依赖等时序关系，并生成可时序推理的知识图谱。

主要指标：（1）提出基于文本、图像、视频等多模态数据的时序知识图谱建模方法与时序知识抽取算法，时序知识抽取精度相比 sota 有 5%左右的相对提升；（2）在提出的时序知识图谱建模与抽取方法的基础上，在智慧教育、智能制造等领域实现完整的时序知识图谱抽取与推理系统，并交付相应可复现代码和方案；（3）发表或录用高水平论文 2 篇，申请国内发明专利 3 项。

5.面向领域知识中不确定性问题研究

研究内容：复杂领域场景涉及知识维度广，业务专家基于领域知识（经验）在短时间内做出的评判具有很强的主观性。与此同时，由于复杂领域场景中获取的数据源与领域知识之间的知识抽取过程中，存在数据源的固有的不确定性问题，由此导致通过其抽取的领域知识以及基于领域知识的应用任务实现的不确定性问题。目前，面向领域知识中的不确定性问题尚未解决，也是复杂领域场景中亟待解决理论

难题。本指南旨在研究面向领域知识中不确定性问题，构造一种可以量化不确定性的领域知识图谱，从而为复杂领域场景提供对相关概念的规范化、明确化描述，为知识的共享打下了基础,为领域知识的组织和构建提供了一个良好的平台。

主要指标：（1）提出复杂领域场景中领域知识的不确定性量化模型；（2）提出基于不确定性量化模型的领域知识图谱表示方法；（3）构建复杂领域场景的通用领域知识图谱平台;（4）发表或录用高水平论文 3 篇，申请国内发明专利 3 项。

（二）面向科学研究的智能计算

1.农作物快速基因编辑体系研究与应用

研究内容：开展农作物多基因编辑技术、病毒介导基因编辑技术或不依赖基因型的基因编辑技术研究，建立高效基因编辑育种技术体系，辅助主要农作物关键基因功能的高通量验证和相关功能品系获得。

主要指标：（1）建立一套面向主要农作物的快速基因编辑体系；（2）为基于智能计算、表型组分析所获得的关键候选基因进行功能验证分析。

2.农作物空间代谢大数据挖掘方法与应用

研究内容：开展农作物高通量空间代谢组学数据挖掘和分析，研究植物生长发育密切关联的空间代谢网络调控技术，建立空间代谢组学数据库及三维立体模型，通过智能计算获得影响品质的关键代谢物。

主要指标：（1）研究高通量空间代谢组数据分析技术，提高分析效率；（2）建立空间代谢物三维立体模型；（3）获得影响品质的关键代谢物。

3.智能材料复杂体系智能计算算法和程序

研究内容：针对智能材料多场耦合问题，发展复杂体系的机器学习表征和代理模型加速计算方法，撰写 GPU 加速的高通量计算程序，研究热-力-化学耦合对智能材料微观组织的影响规律，构建微观结构与宏观性质之间的关系，为发展高性能智能材料提供设计准则。

主要指标：发展智能材料复杂体系多场耦合的机器学习表征方法和代理模型方法,实现显著优于传统计算方法的计算加速比；开发融合机器学习算法和物理理论模型的 GPU 计算程序；提供智能材料设计准则 1 条以上。

4.材料设计的多尺度方法与软件工具

研究内容：基于材料基因工程的研究范式，针对材料在微观、介观和宏观尺度下不同的行为与特性，利用第一性原理计算、分子动力学、相场理论和有限元分析等，发展多尺度的高通量材料计算方法，开发高度自动化的材料计算数据成、存储和分析的程序软件。

主要指标：集成不同尺度材料计算方法，对批量生成的材料结构进行高度自动化的计算模拟；不同尺度功能模块之间实现有效连接，为开展新材料设计，提供专业化方法与软件；完成基于第一性原理、分子动力学和相场模拟集成计算的材料设计软件 1 套。

5.药物分子与靶标蛋白亲和力预测分析

研究内容：开展对隐式溶剂模型的两点式自由能计算方法及其应用的研究，研究以异质化溶剂模型替代传统的均一化溶剂模型的自由能计算方法，研究结构水分子存在的情况下对药物分子与靶标蛋白亲和力的快速准确预测方法。

主要指标：（1）建立结构水分子数目及位置预测的机器学习模型；（2）建立新型异质化模型及自由能预测方法；（3）一套结构水分子的建模与优化工具软件。

6.基于数据挖掘的新型 Cas 蛋白功能特征的研究与优化

研究内容：开展对新型 Cas 蛋白工作机制的探索，研究 Cas 蛋白高效、特异的识别和切割能力的优化方法，分析蛋白-核酸相互作用位点、相互作用的实时动态影像、R-loop 形成的特性、对核酸进行结合或切割特性

主要指标：（1）单分子解析新型 Cas 蛋白工作机制；（2）新型 Cas 蛋白的优化方法。

（三）新型智能计算理论、架构与方法

1. 基于脑启发的类人智能研究

研究内容：探索大脑对记忆是如何进行存储和检索；探索睡眠对大脑的学习记忆提高以及清理内存空间的机制；结合睡眠在记忆巩固以及清理内存空间上的作用，开发睡眠启发的可持续学习的类人智能模型，并验证模型的准确性。

注：本项不设具体指标。

2. 面向新型存储器类脑芯片实现的硬件-算法协同优化设计

研究内容：研究适用于新型存储器类脑芯片的高鲁棒性脉冲神经网络算法以及硬件操作方法；构建新型存储器（例如忆阻器等）器件仿真模型并研究针对器件非理想因素的补偿算法和电路补偿方案；研究脉冲神经网络算法到新型存储器阵列的映射方案；针对新型存储器的原位可编程优势提出适配的局部可塑性学习算法并引入全局调控机制；研究量化误差对网络性能的影响规律并研究精度自适应的实现方案。

注：本项不设具体指标。

3. 面向高速光场处理的光电计算架构研究

研究内容：面向未来自动驾驶、机器视觉等场景中的高速光场信号处理需求，针对光学递归神经网络在图像信号处理过程中的带宽瓶

颈，研究新型光学神经网络计算架构，探索软硬件协同处理机制，搭建可编程光电计算系统，实现高能效的光电混合计算。开发高帧率图像识别算法，演示高速图象识别任务，实现光场信号的高精度实时处理。

主要指标：（1）计算能耗 3TOPS/W 以上；（2）支持分辨率为 128×128、224×224 的图像输入；（3）对应处理帧数分别不低于 500、300 帧；（4）在 MNIST 数据集上正确率不低于 95%，在 Human action recognition（Weizmann and KTH databases）上正确率分别不低于 99%和 95%。研究成果在相关国际顶级期刊发表 1 篇论文，申请国内发明专利 1 项。

4.基于图计算的高效分布式异构内存系统

研究内容：面向大规模复杂图计算应用场景，支撑数据高效存储、分布式内存共享、数据快速索引、资源分离管理等问题；研究并开展实际任务场景下的基于图计算的数据分布式内存存储、管理、共享等关键技术；基于之江自研的高并发分布式图计算系统，构建分布式存储平台和分布式数据共享架构。

主要指标：（1）实现支持图计算的分布式异构内存池系统，提供高效的分布式内存访问；（2）实现支持图计算的异构内存键值存储系统，提供高吞吐访问性能；（3）实现基于分布式异构内存池的持久化通信系统，保证分布式异构内存系统的可靠性；（4）提出基于异构内存的磨损均衡策略，保证异构内存系统的可靠性和寿命；（5）探究分

离资源管理系统的智能网卡优化机制，提出有关问题，形成设计思路；（6）研究成果在相关国际顶级期刊发表至少 2 篇论文。

5.广域异构计算资源最优协同调度方法研究

研究内容：面向异构计算资源的分布式调度与资源监控系统，研究通过实时资源监控优化跨平台任务调度，提升集群资源配置效率的技术方法。包括研究异构计算资源的抽象模型，实现云际、多云等广域场景的资源描述模型；研究跨平台的计算优化技术，实现跨平台的计算流程智能调度、跨平台计算流程智能监控；研究广域的异构多平台任务部署技术，实现基于容器的多任务、多管道智能部署。

主要指标：形成广域异构资源的抽象描述能力模型，支持能耗相关的抽象指标；构建支持多策略调度模型，策略数量大于 5 种；研究成果在相关国际顶级期刊发表或录用论文 1 篇，申请国内发明专利 1 项。

6.基于液晶超表面的全光神经网络研究

研究内容：旨在建立一套全光神经网络系统，通过使用液晶超表面来模拟衍射神经网络的每一个衍射层。根据神经网络预定的任务目标，选择对应的损失函数，并通过模拟计算反向传播的方法指导动态调控每一个液晶超表面单位相位、振幅等关键参数。最终，借助全光衍射神经网络对入射光场进行识别，实现光学衍射神经网络的学习能力。这种光学衍射神经网络可以实现类似于计算机上神经网络的学习

能力，实现对输入信号的直接光学分类或拟合等函数功能。其功耗较传统电学神经网络将降低一个数量级，其速度至少为传统电学神经网络的 3 倍以上。

主要指标：（1）通过液晶超表面的制造工艺提升，实现超薄液晶超表面（约在波长量级），并可在此超薄距离内完成 2π 的相位调控；（2）通过多片超薄液晶超表面的叠层设计，实现全光神经网络系统，实现对 MNIST 和 FashionMNIST 等标准数据集准确分类能力，其分类准确率达到 95%以上，训练时间相较传统电学神经网络减少 30%以上，能耗降低一个数量级，速度提高三倍以上；（3）探索全光神经网络在更复杂的任务背景下的功能实现可能性，例如病理图片等医学图像的快速处理等。结合之江实验室已立项“面向快速、精准术中病理诊断的新型激光超声传感成像”项目，实现光声病理图片影响的高速识别判定（判定时间小于 1 分钟），解决术中病理等医学图像诊断过程中的瓶颈关键问题。

（四）类人五感与多维感知

1.仿人视觉的人工智能算法研究

研究内容：研究具有仿人视网膜至视觉皮层 V4 区结构的人工智能算法。结合人类视觉的生成原理，研究人类大脑视觉皮层各层次输出特征的表达方式，由图像构建相应的特征，形成数据集。根据上述特征生成方式，以生物学原理作为约束，研究参照人类视觉生成过程的具有阶段性约束的成像算法，构建出具有仿人视神经的神经网络模型。

主要指标：（1）提出/构建出具有仿人视网膜至视觉皮层 V4 区结构的神经网络模型，建模过程需参照人类视觉生成过程，阶段性约束模型成像。（2）配合之江实验室相关团队的需求改进模型，以类人视觉特征输出（轮廓、角点、方位、运动方向等）形式实现视觉生成，网络总层数不高于感光细胞到 V4 区神经网络层数的 3 倍。

2.基于生物计算的嗅觉知识挖掘技术研究

研究内容：利用生物计算方法，建立基于基因序列的嗅觉受体蛋白三维结构和气味结合功能计算方法；针对目标气味分子检测，研究嗅觉受体蛋白的三维结构和基因序列设计方法；挖掘并建立嗅觉受体蛋白的基因序列、三维结构、气味结合功能之间的关系，为构建嗅觉知识库以及实现类人嗅觉系统提供技术支撑。

主要指标：（1）基于基因序列计算得到嗅觉受体蛋白三维结构10种及以上，准确率高于90%；（2）基于10种嗅觉受体蛋白的基因序列、三维结构，形成1种气味结合功能计算方法，准确率高于90%；（3）面向特定气味分子检测，形成1种嗅觉受体蛋白的结构和基因序列反演设计方法，并完成1种蛋白的设计和功能计算；（4）1份研究报告，提供上述计算方法的技术细节及相关代码，并分析总结嗅觉受体蛋白的基因序列、三维结构、气味结合功能三者之间的关系。

3.基于TFT技术的超声换能器设计及制备工艺研究

研究内容：研究基于TFT基底的超声换能器的设计、加工以及微系统集成；研究超声换能器的压电薄膜材料以及电极材料的设计优化与微加工技术；研究超声换能器的驱动与读出电路系统的设计；研究超声换能器阵列在医疗健康等领域的应用设计。

主要指标：（1）提出基于TFT基底的超声换能器加工工艺流程1套；（2）优化加工工艺以及换能器设计，实现2种不同频率的超声换能器；（3）实现基于超声换能器的超声传感验证，像素尺寸500x500μm。（4）申请国内发明专利1项。

4.面向阵列化、多模态智能感知的TFT电流读出基板研制

研究内容：基于之江实验室建设的TFT工艺线研究a-Si TFT的背板设计，以类人五感器件或超声换能器的读出为典型应用案例，设计一套电流输出器件的阵列读出基板，并在之江实验室TFT工艺线具

备条件后在之江实验室实现流片，并实现类人五感传感器或超声换能器阵列传感信号的读出验证。

主要指标：（1）TFT 电流读出基板：数量≥2 套，阵列规模≥250×350（真实采集区）；（2）像素截距≤90μm^2，形成完整的设计图纸 1 套。

5.单光子超快信号探测

研究内容：针对高灵敏、超高时间分辨率（< 1 ps）光学信号测量难题，研究基于单光子时间分辨光谱测量（single photon time-resolved spectroscopy）与相位恢复（phase retrieval）方法的单光子超快光学信号测量与表征技术。为突破量子噪声局限，开发基于神经网络等人工智能算法的相位恢复算法，实现对微弱信号复振幅（振幅+相位）的快速测量。

主要指标：（1）基于二维阵列式 SPAD，设计原型系统方案，探测光学信号复振幅（complex amplitude），时间分辨率< 1 ps.（2）相位恢复算法重构速度< 100 ms.（3）发表或录用高水平论文 1 篇，申请国内专利 1 项。

（五）智能网络

1.基于多模态网络环境 PINE 的网络模态创新与验证

研究内容：面向智能计算、工业制造、能源与低碳等垂直行业应用需求，突破现有 TCP/IP 技术体制在编址/寻址、协议体系、路由控制、交换模式、传送方式等基线方面的能力约束，基于多模态网络环境 PINE 开展网络模态创新和应用研究，设计与垂直行业应用适配的新型网络模态，提出其寻址、路由、转发、安全等运行逻辑和协议机制，给出其应用场景设计或部署案例，并通过与现有网络技术体制进行对比分析新型网络模态的功能/性能优势。

主要指标：（1）针对一项或多项垂直行业应用需求，提出一套新型网络模态设计方案，包括其运行逻辑、协议机制、应用场景等，完成原理验证（依托自有环境或基于之江实验室已有多模态网络环境），对比分析技术指标不少于 2 项；（2）发表或录用 JCR 二区（含）以上论文不少于 2 篇。

2.可编程智能计算网络一体化编译技术

研究内容：研究可编程智能计算网络一体化编译系统架构和运行逻辑，明确各模块之间的交互机制和接口关系；突破当前分别对数据平面、控制平面进行编程的现状，设计面向数据平面和控制平面的一体化功能抽象模型和形式化描述方法，支持网络功能灵活可定义；研究网络功能与数据平面、转发平面资源的高效映射机制；开展原理验

证（依托自有基础或基于之江实验室已有多模态网络环境）或研发编译原型系统。

主要指标：支持计算、转发、存储、安全等可编程，支持网络程序跨平台移植，支持基于网络状态和平台能力评估的网络程序编译和部署，支持模块化编程和增量式编译。针对不少于 3 种网络模态开展实验，涵盖智能计算中的计算、存储、转发、安全等编程场景。

3.面向对抗攻击的异构神经网络构造技术研究

研究内容：研究面向对抗样本的神经网络模型异构性定量评价体系，提出模型异构性评价指标并验证其有效性；研究高异构性神经网络模型构造技术，从同一个基模型批量生成具有高异构性的神经网络模型集合。

主要指标：提出不少于 2 种有效的神经网络模型异构性定量评价指标；在同构模型上具有迁移性的对抗样本中，在异构模型上迁移成功率降低到 10%以下；与其他异构模型构建方法相比，迁移成功率降低超过 20%。

4.基于 AI 的模糊测试技术研究与实现

研究内容：针对当前模糊测试工具种子选择算法效率低下，路径覆盖率低等问题，运用人工智能的方法对现有模糊测试工具进行改进，主要完成被测软件测试用例有效输入的筛选、种子智能化变异、种子队列快速选取、以及人工智能算法同模糊测试工具的高效交互等

方面的研究，突破当前种子选择策略死板，有效变异种子生成效率较低等难题，实现对现有模糊测试工具效率的大幅提升。

主要指标：（1）针对当前主流数据库软件，Web 相关软件进行测试，软件数量不少于 5 款；（2）针对 AFL 工具 havoc 阶段种子变异效率提升 5%-10%；（3）路径覆盖率提升 30%-40%。

（六）声学实验室

1.复杂场景下基于声纹识别的定向人声分离研究

研究内容：人声分离是鸡尾酒会问题中一个比较难的分支。在多人会话环境下，基于个性声纹的语音识别是实现人声分离的其中一个解决方案。构建基于听觉信号和视觉信号的目标语音包络、基频等关键特征的精准解码技术，确定听觉系统在多说话人环境中所关注的目标语音；探究听觉注意力指导下的目标声纹精准感知技术，构建基于目标语音特征解码结果的多模态目标语音提取算法，通过融合多模态信息以提升复杂声学环境下目标语音的感知质量，实现真实场景中精准的人声分离。

主要指标：（1）基于多模态信号的目标说话人判定准确率不低于90%；（2）目标语音感知质量（PESQ）不低于 2.8；（3）多模态目标语音感知算法延迟不高于 20ms；（4）基于声纹的人声分离SDR(source-to-distortion ratio)不低于 18dB；（5）申请发明专利2 项，发表高水平论文 1 篇。

（七）双足机器人

1.人形机器人拟人化全身运动技巧学习算法与仿生多层控制系统研究

研究内容：面向人形机器人拟人化全身运动与基本作业要求，研究类人的运动技巧迁移与学习算法，探索并开发融合深度强化学习与序列优化控制的、先进的多层控制框架；基于深度强化学习，提取机器人与环境交互的技能集及建立动作基元库；基于序列优化控制，研究高动态响应下的全身运动实时协调优化控制与上下肢平衡稳定控制；在人形机器人动力学系统上，实现多点接触、强环境作用下的人形机器人类人操作与全身柔顺运动。

主要指标：（1）建立融合深度神经网络与序列优化控制的仿生多层控制系统，在人形机器人样机上实现全身的实时协调运动控制；（2）实现与环境多接触下，不少于 4 点接触的全身实时协调控制；（3）实现手臂不低于 2Hz 挥动情况下的全身稳定控制；（4）面向家居与导览场景完成不少于 3 项的作业场景仿真验证，实现类人技巧的迁移与学习，达到上下肢协调运动与移动作业需求；（5）发表高水平论文 1-2 篇。

2.具有扰动自恢复及地形自适应能力的仿人机器人腿部机构

研究内容：面向具有扰动自恢复能力的仿人机器人腿足机构结构设计，研究仿人机器人腿足物理特性与运动平衡能力的关联关系，研

究机器人腿足机构结构与扰动自恢复能力的评价模型构建方法，提出具有一定抗干扰能力及地形自适应能力的刚-柔耦合仿人机器人腿足机构构型设计方法；研究高强度、低惯量的仿人机器人腿足机构尺寸综合与驱动优化布置方法；研究轻量化腿部拓扑结构优化方法，实现在满足自适应、抗干扰行走前提下的腿部轻量化优化设计。

主要指标：（1）至少提出两种腿部结构设计构型方案，具备平地、沙地、碎石等不少于 3 种场景下的稳定行走能力；（2）非主动控制情况下，抗瞬时冲击能力大于 0.4 N×S/KG；（3）申请国内发明专利 2 项，发表高水平论文 1-2 篇。

3.基于人体运动力学数据驱动的腿-足协调机理解析与运动能效调控研究

研究内容：面向仿人机器人应用，开展融合关节轨迹-足底力-肌电多物理信息的人体运动力学试验；建立基于数据驱动的人体下肢肌腱-骨骼一体化归约建模与动力学行为研究；探索人体运动的腿-足协调机理解析与能效调控机制，开发人体肌腱-骨骼系统的协同运动模拟系统，获取人体腿-足的运动-力-刚度协同调控规律，为构建人体运动基元模板提供原始数据积累，为未来高性能仿人机器人研制提供设计参考。

主要指标：（1）开展人体行走、奔跑、跳跃至少 3 类的运动生物力学测试，同步采集下肢腿-足的运动轨迹、肌电信号和足底力的时间历程数据；（2）建立人体下肢肌腱-骨骼一体化数学模型，开发人

体运动模拟程序，模拟稳定步行（不小于 1m/s)、奔跑(不低于 3m/s)、跳跃(不低于 1.5m)等三种运动；（3）建立人体下肢腿-足的运动-力-刚度协同调控方法，再现人体自然运动形式，并进行仿人机器人仿真验证；（4）发表高水平论文 1-2 篇。

4.机器人通用多模态知识表达和计算

研究内容：面向导览、家居等场景的机器人自主作业需求，研究基于多模感知信息的机器人知识通用表达和计算方法，研究基于符号和向量空间的混合推理理论和算法。

主要指标：研究机器人通用多模态知识表达和计算框架，可对导览、家居等场景中机器人所面对的多种模态知识进行表达和跨模态计算，支撑具体场景下至少 2 项机器人作业任务的自主决策，相关研究成果发表顶会顶刊论文 1-2 篇。

（八）密码学与隐私计算

1.基于多平台的抗量子密码算法工程化实现

研究内容：针对量子计算技术对传统公钥密码体制所带来的潜在安全性威胁问题，本指南拟针对 NIST-PQC 标准化的抗量子密码方案，研究设计面向多平台的高效实现方法。具体地，通过深入分析研究抗量子密码算法中的核心运算，如多项式乘法、模乘算法等，并结合目标平台的架构、内存等特性，给出相关运算在目标平台上最优的实现方案，使得抗量子密码算法在目标平台上的实现性能达到或超过国际领先水平。

针对全同态加密方案计算复杂度高、控制逻辑复杂等工程化时所面临的关键科学问题，当前主流的基于 CPU 软件库的工程实现方式计算效率并不理想。本课题拟通过设计基于并行计算架构的专用加速模块来加速底层关键算子的计算速度和并行计算吞吐量（NTT、RNS 等），最终搭建异构计算平台来解决全同态加密的计算效率问题。

主要指标：在至少 1 种平台上（ARM、FPGA 等）完成 2 种以上的抗量子密码算法实现，与同类官方参考实现相比相关密码算法整体效率提升 30%-50%。提交一套能通过功能验证的抗量子密码完整代码工程库，包含至少 2 种算法，以及相应的使用说明和性能测试报告；在至少 1 种并行计算平台上（FPGA、GPU 等）设计和实现 NTT 专用加速模块，计算速度相比主流软件库实现（SEAL、HElib 等）提升至少 5 倍，全同态加密整体性能相比主流软件库实现（SEAL、HElib 等）提

升至少50%。提交一套能通过功能验证的全同态加密异构计算工程库，以及相应的使用说明和性能测试报告；投稿或发表相关高水平论文（IACR七大会议或CCF-A/B类会议期刊或IEEE/ACM期刊）至少3篇。

2.面向去中心化联邦学习的规则引擎设计与实现

研究内容：为支持学习过程安全和数据隐私保护的去中心化联邦学习，设计并实现基于区块链的规则引擎系统，包括适合联邦学习的区块链高效共识算法、弹性分布式数据存储架构以及学习规则的智能合约方案。

主要指标：要求参与的分布式节点不小于3个；系统能防范最多1/3恶意节点，每一轮共识处理时延不大于10秒，原型系统能支持不少于5个节点；能够至少完成2种学习任务；提交能通过功能验证的去中心化联邦学习原型系统的完整代码工程库，以及相应的使用说明；投稿或发表高水平论文（CCF-A/B类会议期刊或IEEE/ACM期刊）至少3篇。

3.基于空中隐私计算的联邦学习研究

研究内容：针对传统联邦学习系统面临的通信开销大、难以规模化等瓶颈问题，引入模拟空中计算进行联邦模型训练、以提高系统的通信效率；同时，利用参数在模拟传输过程中引入的信道衰落和噪声提升联邦学习模型的隐私保护能力，实现强隐私、大规模的联邦学习机制。

主要指标：与基于传统调制解调与数字化传输方案的联邦学习方法相比，通信效率提升 20%以上，隐私保护增益提升 10%以上，性能降低不超过 5%、甚至可提升原有联邦学习方法的性能。提交功能性验证通过的完整代码，以及相应的使用说明文档；投稿或发表相关高水平论文（CCF-A/B 类会议期刊或 IEEE/ACM 期刊）至少 3 篇。

4.基于轻量级隐私保护的联邦学习研究及激励机制设计

研究内容：针对联邦学习中面临的典型隐私威胁，本课题拟构建基于隐私计算的联邦学习隐私保护方案，设计基于轻量化隐私保护协议以及参与者隐私保护激励机制，并在满足对联邦学习模型性能影响较小的情况下，实现学习场景的隐私增强。

主要指标：基于隐私计算的联邦学习隐私保护方案对联邦学习准确影响不大于 10%，原型系统能够抵御不少于 2 类典型的联邦学习隐私威胁。投稿或发表高水平论文（CCF-A/B 类会议期刊或 IEEE/ACM 期刊）至少 3 篇。

5.分布式多方计算平台代码漏洞检测与数据隐私保护关键技术研究

研究内容：针对多方计算平台智能合约代码可能存在安全漏洞导致的多方计算公平性、安全性面临威胁的问题，研究基于抽象语法树与语义图构建的代码静态安全分析方法，研究基于前瞻分析与模糊测试的动态模糊测试技术，研究基于深度学习的种子变异与路径权重分

配算法，切实保障分布式多方计算平台智能合约代码在产业应用中的程序安全。针对分布式多方计算平台因多方共享数据或参数导致的隐私泄露问题，研究多方计算平台和产业应用中的数据隐私保护技术，研究联邦学习中的差分隐私保护技术，实现分布式多方计算平台的数据隐私保护。实现数据安全性能或代码漏洞检测准确率达到或超过国际领先水平。

主要指标：提供隐私保护与智能合约代码漏洞检测技术报告；提供开源的分布式多方计算平台智能合约代码安全漏洞检测算法代码一套，实现对可重入、整数溢出、时间戳依赖等不少于 5 类安全漏洞的检测；投稿或发表代码安全、隐私保护等方向的高水平论文（IACR 七大会议或 CCF-A/B 类会议期刊或 IEEE/ACM 期刊）至少 3 篇。

6.隐私计算下的机器学习算法信息发布技术研究

研究内容：机器学习技术已经被广泛应用于生产生活中。但在带来巨大的社会经济效益同时，机器学习技术正面临着日益凸显的数据隐私风险。当前研究结果表明，未经保护的机器学习算法输出可能会引发训练数据泄露、模型信息窃取等隐私安全问题。对此，本课题拟探索基于隐私计算的机器学习算法测试技术。具体地，评估主流机器学习算法的隐私泄露风险，确定潜在的隐私泄露形式；研究机器学习算法输出信息与隐私泄露程度之间的关系，分析在机器学习算法开发和部署阶段进行隐私保护的可能性；在隐私计算场景下，设计机器学习测试方案，以评估机器学习算法输出信息引发的隐私泄露风险。

主要指标：形成一套机器学习算法隐私泄露风险评估框架，支持对训练数据泄露等问题的分析测试；在至少 2 种数据集上，对不少于 3 种主流深度学习模型的隐私泄露问题进行测试分析；提交一套机器学习算法隐私泄露风险测试评估算法实现代码，以及相应的使用说明；投稿或发表高水平论文（CCF-A/B 类会议期刊或 IEEE/ACM 期刊）至少 3 篇。