附件 1

国家网络空间安全国家科技重大专项
第二批项目申报指南

2.1 关基商用密码安全检测评估技术及应用示范

研究目标: 针对典型关基场景密码应用中存在的合规性不足、缺陷难发现、运行状态不可视等短板问题，以及不同行业、不同类型关基密码应用与安全检测评估的差异化需求，重点突破密码应用缺陷自动化检测、密码资源勘探与运行图谱构建、安全态势感知与应急处置等关键技术，构建覆盖关基密码应用全过程、可追溯可审计的密码应用安全检测评估技术体系，形成对数据加密、身份鉴别、电子签名、密钥管理等典型关基密码服务运行时功能正确性、有效性及持续性的全面感知和快速处置能力。

研究内容: 研究关基密码安全检测评估技术体系。研制通用型及离线检测、动态检测、集成性测试等新型密评工具。结合网络流量、代码、日志、数字证书等多种方式，实现关基密码应用环境中密码设备、应用系统、关联业务等密码资源的勘探与图谱绘制。研究关基密码安全威胁与应急处置对抗模型和关键技术，实现典型密码服务运行状态监测预警。研究关基关键密码支撑和业务功能模拟仿真技术，建设关基密码应用典型场景仿真测试平台，为关基密码安全应用提供体系化仿真测试环境。在重点行业

开展综合应用示范。研究数据加密、身份认证电子签名、时间戳、密码资源池、密钥管理等典型密码服务在运行时的功能正确性、安全性、合规性等检测评估技术形成智能化商用密码运行安全监管平台体系化技术链，支撑关基商用密码应用全时动态评估、预警监测和应急处置。

考核指标： 形成 1 套关基密码安全检测评估技术体系框架，以及 1 套关基运行安全技术体系框架。编制 3 个国家或行业标准。研制新型密评工具集，支持源代码静态检测及二进制代码动态非侵入式检测，支持检测不少于 50 种密码应用缺陷，准确率不低于 95%。攻克 3-5 项商用密码运行安全监管关键技术。研制 5 款以上密码应用安全性评估工具。研制关基密码资源勘探与图谱绘制平台，实现密码设备、应用系统、关联业务等密码资源的勘探与图谱绘制。研制关基密码应用安全态势感知与应急处置平台，支持不少于 3 种典型操作系统密码服务运行时的状态监测预警。建设关基密码应用典型场景仿真测试平台，支持不少于 5 个场景仿真测试。在不少于 5 个关基行业中开展综合应用示范。

实施期限： 3 年

立项要求：支持 1 个项目，采用公开竞争方式。由具有商用密码检测机构资质证书的单位牵头申报。

中央财政资金支持方式： 事前立项事前补助。配套资金与中央财政资金不低于 4:1 匹配。

2.2 关键数据跨域协作的隐私保护技术及应用示范

研究目标: 针对关键数据跨域协作场景中数据知识提取与利用过程中面临的隐私泄露等风险，突破跨域数据知识提取与融合互通、高性能密态计算、协作监控与审计等关键技术，研制数据跨域协作的智能隐私计算平台，为跨域数据的安全利用与协作提供系统性技术方案与示范性落地平台。

研究内容: 面向不可出域数据的跨域协作场景，研究原始数据不出域、知识可共享的分布式跨域数据知识提取与联合建模框架，突破异构多模态数据的高效知识提取、多源异构知识传递与融合隐私保护、隐私保障下的跨域数据持续性知识积累与集成、数据可用不可见的联邦查询与学习等技术; 研究软硬件协同的高性能隐私计算技术等; 研发数据跨域协同隐私计算安全基座，突破多源异构数据要素跨域协作的可信监管与可量化验证审计、异构隐私计算系统互操作中间件、数据-模型-算力联合调度引擎、抗量子安全隐私计算、隐私计算软件栈安全分析技术等关键技术; 研究广域异构、自主可控、通用可编程的高性能隐私计算平台。

考核指标: 基于商用密码构建面向金融、通信等国家重要行业的跨域数据协作隐私计算系统，制定跨域数据隐私计算国家、行业或团体标准（草案报批稿）不少于 2 项，建成面向国家行业数据的广域异构高性能隐私保护计算平台，计算节点分布式部署不少于 5 个省数据中心，超 1000 公里跨广域网计算节点往返网络延迟不低于 20 毫秒，隐私计算单次调用平均响应时间小于

30ms，平台日均数据处理能力不低于 10TB，并在国家重要领域进行示范应用；实现数据不出域的多机构联合知识共享与建模能力，跨域分布式模型性能提升不低于 10%；实现知识融合与利用过程中隐私强化机制的理论可证性，确保不可信环境中恶意破坏的检测成功率超过 90%；密态计算平台兼容国产主流人工智能加速硬件与 CPU 硬件，支持不低于 20 种智能模型结构；相比于明文智能模型计算，密态智能计算性能损失小于 10 倍，精确度损失小于 1%；支持可信计算环境全计算过程特权攻击检测，平均攻击漏检率低于 1%；实现不少于 3 种异构数据要素的跨域协作监控，监控覆盖率达 99%以上，异常协作识别率达 95%以上，并确保监管决策的可验证性；日志抗篡改，审计响应时间达秒级；实现不少于 2 种异构隐私计算系统的互通联动；联合调度引擎提升跨域数据隐私计算性能 15%以上。

实施期限： 3 年

立项要求： 支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式： 事前立项事后补助。配套资金与中央财政资金不低于 4:1 匹配。

2.3 多模态信息传播认知影响致效评估分析技术及应用示范

研究目标： 围绕网络空间内容治理需求，研究认知致效与网络传播建模共性技术，揭示网民认知影响致效要素，研究社交关系与社会属性对个体和群体的认知影响规律，建立多维认知影响

模型；研究网络传播算法的认知影响评估技术，评估网络信息在传播过程中的认知影响。为科学、精准、动态的评估多模态网络信息传播认知影响提供技术支撑。

研究内容：研究多模态信息认知影响要素分析与量化表征、多模态信息特征与认知影响要素映射归因等技术，以信息为中心对认知影响要素进行度量；研究信息传播通道和传播方式对网民的认知影响致效技术，揭示大规模、多尺度复杂传播网络动态演化机制，对网络传播中的信源、链路、受众等多维要素进行评估与分析；研究社交关系和社会属性对个体和群体的认知影响，建立科学、可量化的认知致效评估模型，实现对认知影响要素、路径和作用强度的智能计算；研究基于因果推断的网络信息推荐技术，实现多主体、多目标、多层级的认知传播致效策略生成；构建多模态信息传播认知致效实验验证平台，在经济、社会、文化传播等典型场景对认知影响致效关键技术进行评估验证。

考核指标：支持文本-图像-音频至少 3 种模态组合的因果路径建模，支持对不少于 4 种认知影响要素的分析和量化表征，包括注意力、认知强度、情感唤醒、行为决策等；提出不少于 5 种融合心理学和神经科学的多模态信息认知影响智能算法模型；构建复杂网络的认知传播致效量化评估方法，覆盖形象塑造、认知扭转等不少于 3 类认知影响场景，复杂网络的认知传播致效评估关键特征不少于 200 个；支持认知传播致效策略自动生成，策略

有效率不低于 80%; 构建个体认知度量指标体系，个体认知能力评估预测准确率不低于 85%; 研制多模态信息传播影响认知致效实验验证平台，形成网络传播算法认知影响度量模型和治理技术工具集，在相关重点行业或领域开展技术验证及应用示范。

实施期限： 3 年

立项要求：支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 3:1 匹配。

2.4 新型网络社交场景识别与恶意行为监测预警技术及应用示范

研究目标： 针对网络动态社交场景表征识别难、潜在隐蔽风险推理挖掘难、动态环境行为模式和身份溯源验证难，以及隐匿社交网络识别难、协同监测预警能力不足等问题，突破面向新型社交平台架构、用户行为模式、内容传输规律及识别分析等技术，提升新型网络社交场景识别与恶意行为监测预警能力，为有效阻止新型网络社交场景的恶意行为提供技术支撑。

研究内容： 研究新型网络动态社交场景采集识别分析模型，研究新型社交场景架构、用户行为模式及内容传输规律，隐匿网络新型社交行为分析；研究构建新型社交场景特征刻画指标；研究网络动态社交场景识别与分析、新型社交场景特征构建与边界识别技术；研究时空关联的恶意和违法线索与行为模式挖掘、跨

平台违法行为识别与追踪定位、社交场景虚实身份关联发现等技术；研制新型网络社交场景识别与违法行为监测预警原型系统并进行应用示范。

考核指标：研制新型网络动态社交场景采集识别分析系统，可针对不少于10种境内外常用APP商店，新型社交属性APP、小程序及社交应用软件等社交场景的发现准确率超过90%，实现对新出现的社交场景的动态监控，出现到发现的时间少于24小时；构建新型社交场景多维特征刻画指标体系，覆盖不少于50个维度；构建新型社交APP或应用软件场景检测工具，新型社交场景边界检测识别准确率大于80%，支持隐匿网络社交场景不少于5种，社交行为识别率大于80%；面向不少于10种违法行为，构建线索与行为模式挖掘及追踪模型库，模型数量不少于100个，跨平台违法行为追踪监测准确率超过90%，境内平台主体真实身份定位准确率大于80%；研制新型网络社交场景识别与恶意行为监测预警原型平台，支持不少于5种语言，在相关重点行业或领域开展技术验证及应用示范。

实施期限：3年

立项要求：支持1个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于3:1匹配。

2.5 面向认知安全的内容可控生成技术及应用示范

研究目标: 针对多模态内容生成技术在认知安全领域存在的跨模态语义控制粒度不足、生成内容与目标认知规律脱节、高质量人机协同创作低效等问题，开展多模态内容细粒度可控生成与编辑技术研究，突破跨模态语义对齐、内容可控生成、人机交互式编辑、局部内容优化、生成质量评估等关键技术，有效提升多模态内容生成与编辑技术的可控性、交互性、精细化程度以及生成效果评估等方面的能力，增强认知应用场景下的内容生成水平。

研究内容: 研究跨模态细粒度表征与对齐技术，研究多模态语义分解与层次化表征方法，实现跨模态语义要素的细粒度解耦与重组；研究认知效应感知的自适应控制生成技术，实现生成内容安全可靠；研究认知反馈驱动的交互式生成编辑技术，突破全双工自响应式的交互内容生成技术；研究多模态协同生成与编辑的时序一致性保持技术，实现多模态内容的精准编辑与动态重组；研究局部编辑内容优化技术；研究云端协同的批量生成实时响应技术，实现自适应资源动态匹配；研究面向认知安全的多模态内容生成评估体系，突破多模态可控内容生成质量动态评估技术，实现多维度的生成效果有效评估。

考核指标: 形成跨模态特征对齐与解耦模型，支持对多模态信息的情感、语义、音色等细粒度特征的对齐与解耦，准确率不低于 85%；形成交互式的高拟真细粒度微控生成工具集，支持人、物体、场景等元素的精细化编辑，支持不少于 10 种用户认知反

馈驱动的交互式编辑策略，策略调整延迟达分钟级，支持具有自主交互能力的特定内容生成，生成动作相似度不低于85%，具备全双工、自响应功能；构建面向认知安全的多模态内容生成评估体系，覆盖不少于4个维度，不少于16个量化指标；研制多模态内容细粒度可控生成与编辑平台，支持教育、文化等不少于10类特定主题内容的生成和编辑，在相关重点行业或领域开展技术验证及应用示范。

实施期限：3年

立项要求：支持1个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于3:1匹配。

2.6 下一代特种工业互联网安全关键技术及应用示范

研究目标：为提高下一代特种工业互联网安全防护能力，研究下一代特种工业互联网多场景下安全对抗理论及关键技术，突破无人装备科研生产、实网应用场景下的高对抗性新型对抗测试技术，突破下一代特种工业互联网跨域新型对抗检测与对抗增强技术，形成预先抑制攻击、及时检测攻击、协同处置攻击的无人装备体系主动防御能力。

研究内容：研究下一代特种工业互联网多场景业务安全建模与跨域安全风险评估方法，形成无人装备多场景跨域新型对抗机理框架、测试方法与评估体系；研究无人装备科研生产场景对抗

技术，对科研和生产网络的物理域、控制域、供应链等方面实施有效对抗测试，验证数据泄露、系统破坏、生产停滞等效果；研究针对典型特种无人装备实网应用场景下的非法接入、控制劫持、运维失陷等三类关键对抗检测手段，形成链式跨域对抗检测路径，对无人装备的个体和群体造成控制、毁伤等效果；研究下一代特种工业互联网跨域新型对抗检测与对抗增强等技术，构建虚实结合的无人装备仿真测试环境，构建特种工业多场景跨域新型防护体系；针对典型无人装备的科研生产、实网应用等场景，开展下一代特种工业互联网安全对抗技术应用示范。

考核指标: 构建下一代特种工业互联网多场景业务安全新型对抗机理框架、测试方法与评估体系；研制无人装备科研生产场景对抗测试平台，覆盖不少于 5 类针对生产环境的投毒方式、6 类对物理域的对抗检测方式，可实现对科研生产环境的数据泄露、零部件投毒、生产停滞等效果；研制典型特种无人装备对抗测试平台，发现不少于 10 个 0-day 漏洞，针对特种领域无人机、无人车、人形机器人、机器狗等无人装备可验证失控或损毁等效果，通过对运维体系渗透，验证无人装备集群指挥阻断、渗透控制或者毁瘫等效果；研制下一代特种工业互联网跨域新型对抗检测和防御平台，支持安全防护策略全局动态调控，至少适配 4 类安全防护设备，支持对不少于 4 种隐蔽跨域对抗检测，构建不少于 4 类无人装备仿真测试环境；在至少 3 家军工企业的科研生产、实网应用环境中，完成研发成果的应用验证。

实施期限： 3 年

立项要求： 支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式： 事前立项事前补助。配套资金与中央财政资金不低于 2.4:1 匹配。

2.7 智能化对称密码分析与设计研究

研究目标： 针对人工智能、大数据和量子计算对传统对称密码带来的新需求和安全挑战，创新智能化密码分析与设计技术，系统化提出新型攻击方法和设计理念，突破现有攻击的能力边界，设计满足新计算场景的分组密码和杂凑函数，产出有影响力的国际标准，为建立国际领先的智能化对称密码分析与设计体系提供技术支撑。

研究内容： 研究基于 AI 的智能化密码分析与检测理论，研究 AI 安全与密码分析的数学和逻辑关联，建立基于密码分析的 AI 安全新理论；研究密码分析技术对神经网络参数安全性的影响，探索神经网络抵抗参数恢复攻击的设计策略；面向新型复杂网络环境，设计满足超低时延、超高吞吐量等性能极限需求的对称密码算法；研究量子计算环境下对称密码新型分析检测方法及高效实现算法，设计高效抗量子对称密码算法；突破大状态分组算法、密码置换的分析瓶颈，研究高效、准确的安全性分析方法；面向海量数据加密需求，研究大状态、超高吞吐量分组密码算法、杂凑函数和带关联消息的认证加密算法的设计方法。

考核指标：融合求解器与 AI 分析技术，构建高效精准密码分析模型和新型密码分析方法，针对系列国际标准算法，相比 SAT 主流求解器攻击轮数取得突破；构建对称密码神经网络与求解器融合的智能化分析检测平台，支持至少 3 种神经网络密码分析方法和 3 种主流神经网络结构的参数恢复功能；设计面向极限需求环境的安全高效对称密码算法，性能相比国际主流算法提升 30%；设计抗量子攻击的超低时延和超高吞吐量对称密码算法，性能相比国际主流算法提升 20%；突破国际杂凑函数和认证加密标准算法分析，提升 ASCON、SHA3 和 SM3 等算法的碰撞与原像攻击轮数；开发针对大状态密码算法的分析工具，对标准认证加密给出突破现有轮数的差分-线性分析区分器；研制量子攻击检测平台，可检测 GFS-2F、GFS-4F 等结构抵抗主流量子攻击的能力。

实施期限：3 年

立项要求：支持 2 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 1:1 匹配。

2.8 新型对称密码分析与设计研究

研究目标：针对高带宽网络流量、内存加密、指令认证、隐私计算、量子安全等新型应用需求，围绕高吞吐认证加密算法、低延迟分组密码算法、隐私计算友好的对称密码算法、抗量子对

称密码算法，构建新型对称密码算法的设计理论，突破安全性分析关键技术，满足高吞吐、低延迟、隐私计算友好、抗量子等应用需求，推进新型对称密码算法的标准化和实际应用。

研究内容: 研究基于 AES-NI 的认证加密算法整体架构，面向高带宽网络流量的应用需求，设计高吞吐认证加密算法；研究低延迟密码部件的构造及硬件电路优化，面向内存加密、指令认证等低延迟应用需求，设计低延迟分组密码算法；研究大素数域和高维扩域多项式理论，构建代数类高效安全分析模型，围绕 MPC、FHE 和 ZKP 等协议设计隐私计算友好的安全高效对称密码算法；研究大状态密码函数的设计理论和分析方法、对称密码安全性分析的自动化和量子加速技术、对称密码的量子电路优化实现及量子安全模型和证明方法，设计抗量子的分组密码和杂凑密码算法。

考核指标: 提出适合高吞吐密码算法的线性层理论，研制高吞吐认证加密算法，吞吐率等软件性能相比国际主流算法提升 20%以上；提出低延迟非线性层设计理论，在同等面积下延迟等硬件指标相比同等规模非线性层低 10%；研制低延迟分组密码算法，在同等面积下延迟等硬件指标相比国际主流算法降低 10%以上；提出低乘法深度隐私计算友好非线性层设计方法，乘法深度相比国际通用算法非线性层低 10%；研制隐私计算友好的对称密码算法，性能相比国际主流算法提升 10%以上；研制抗量子分组密码算法，支持 512 比特密钥及相应安全强度；研制抗量子杂

凑密码算法，支持 1024 比特摘要及相应安全强度。

实施期限： 3 年

立项要求： 支持 1 个项目，采用公开竞争方式。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 1:1 匹配。

2.9 抗量子公钥密码关键技术研究与验证

研究目标： 针对量子计算破解经典公钥密码的严峻威胁，突破我国自主可控的抗量子公钥密码设计关键技术并进行原型验证，研制分析评估系统及工具，提出抗量子公钥密码与传统公钥密码融合应用关键技术并进行原型验证，为建立国际领先的抗量子公钥密码体系提供技术支撑。

研究内容： 研究抗量子公钥密码数学基础理论，包括底层数学困难问题的归约理论、困难问题的经典及量子求解算法，提出新型底层困难问题；研究抗量子公钥密码算法和安全协议的安全高效设计理论与技术，研制抗量子密码算法及安全协议；研究抗量子公钥密码算法和安全协议的攻击和安全性评估方法，建立量子及经典安全性评估模型，研制抗量子密码分析评估系统和工具；研究抗量子公钥密码算法和协议的安全高效软硬件实现技术，基于软硬件实现多个典型抗量子公钥密码系统；研究抗量子公钥密码与传统公钥密码融合应用关键技术，研制兼容主流抗量子公钥密码和传统公钥密码的公钥基础设施原型系统。

考核指标：提出 2-3 个针对主流抗量子密码数学困难问题的求解算法，综合性能指标优于已有算法，突破 1-2 个抗量子数学困难问题求解国际挑战；研制 3-4 个抗量子公钥密码算法，在同等安全强度下综合性能相比 NIST 同类算法提升不低于 10%；研制 1-2 个抗量子安全协议并在 IPsec、TLS 中开展实验验证；设计抗量子公钥密码实现安全评估模型，研制 2-3 套抗量子公钥算法评估软件，实现对基于格、编码、杂凑函数等抗量子密码的安全性及性能评估；设计不少于 2 款抗量子密码算法 IP 核，其中 1 款支持格密码算法且加解密性能超过 500 万次/秒、签名验签性能超过 100 万次/秒、密钥协商性能超过 450 万次/秒；研制抗量子脆弱性检测自动化分析工具，支持传统公钥密码算法的快速定位；研制 1 套兼容抗量子公钥密码和传统公钥密码的公钥基础设施原型系统，面向重要行业或应用场景进行应用验证。

实施期限：3 年

立项要求：支持 2 个项目，采用定向委托方式。由中关村国家实验室作为推荐单位组织有关全国重点实验室申报。

中央财政资金支持方式：事前立项事前补助。配套资金与中央财政资金不低于 1:1 匹配。