附件 **2**

广东省重点领域研发计划 2018-2019 年度“网络信息安全”重点专项申报指南

本专项以国家战略和广东产业发展需求为牵引，瞄准国际最前沿，重点围绕解决大数据安全、网络安全、国产密码技术及设备等，集聚国内优势团队，集中力量联合攻关一批制约产业创新发展的重大技术瓶颈，掌握自主知识产权，制定行业标准，取得若干标志性成果。本重点专项 2018-2019 年度指南共设置大数据安全、网络安全、保密技术及设备、开放性课题等四个专题，专题一至专题三拟支持 9-14 个项目，专题四拟支持不超过 5 个项目。项目实施周期为 3-4 年。

专题业务咨询：文晓芸，020-83163877

专题一：大数据安全（专题编号：0136 ）

项目 1：基于大数据的网络安全态势智能感知关键技术与系统。

（一）研究内容

研究公开信息源网络安全大数据实时采集方法，支持多维度、多层次、全要素无损网络安全采集与提取；构建超大规模网络安全知识图谱，研究基于大数据分析的重大网络事件实时发现与追踪溯源技术，支持对未知攻击的发现。研究基于用户意图理解的智慧解答方案生成技术，支持攻击场景还原和追踪溯源；研究多层次多粒度多维度的网络安全指标体系构建和实时计算方法，支持网络安全评估指数的可配置、实时计算和在线演化。研究自适应、实时的网络安全态势预测技术，支持整体网络安全态势以及重大网络安全事件的快速准确预测。

（二）考核指标

项目完成时须形成一组公开信息采集、调度与评估方法，日采集数量不小于 1 亿条。突破大规模知识图谱的构建与管理技术，构建管理百亿节点、万亿关系的超大规模网络安全及情报知识图谱，知识抽取综合准确率不低于60%，消歧融合的准确率不低于 80%。网络安全事件发现准确度不低于 99%，漏报率不高于30%；支持对全网路由路径图构建与攻击路线还原，支持在非协作网域空间实时追踪定位，能够追踪定位 5 跳及以下的攻击行为；支持不同维度、不同粒度的网络安全态势量化分析，准确率不低于 99%；实现网络安全态势预测，预测准确率不低于 95%。研制软件系统，开展 5 个以上应用，并产生实际应用效果。项目执行期内新申请发明专利或软件著作权 20 项以上，发表高水平

学术论文不少于 10 篇，向国内外标准化组织提交的标准草案不少于3项（其中完成批准立项的不少于1项）。

项目 2：面向大数据应用的隐私保护与对抗技术与方法。

（一）研究内容

研究基于程序浮动的大数据挖掘与隐私保护技术。研究隐私保护前提下的数据分析和模型训练工作台体系结构；研究对自有数据和外部数据源融合分析场景的隐私保护以及数据分析浮动程序的可视化辅助和自动生成技术。研究数据传递中的反隐私隐藏技术。研究基于自然语言处理技术、图像文字检测与识别等智能反隐私隐藏技术，可对包括结构化、半结构化和非结构化数据进行敏感数据识别和脱敏；研究对图片隐写，模型隐藏敏感数据等行为的智能识别与审查；形成可供应用调用和集成的引擎SDK。研究面向数据交易场景的隐私保护技术。研究基于白名单机制的行为和内容审核技术，对数据访问、交易和分析等行为的留痕审计，研发安全的数据交易流转系统；面向政务数据开放场景，聚焦教育、交通、环境、医疗、商业等重点领域，提出适用的数据隐私保护体系。

（二）考核指标

项目完成时须研制完成支持多租户数据隔离与访问控制，支持多租户协同工作流绘制、模型训练、可视化报表生成；支持对自有和外部数据源融合分析场景的隐私保护；支持 3 种以上格式

数据文件导入，亿数量级数据分析结果秒级响应；支持适配 3 种以上主流大数据平台重要组件；支持对数据分析模型的自动化选择与自动化模型参数调优。支持识别常见个人身份信息等敏感数据；支持识别隐匿在大数据平台中的敏感数据，支持识别和还原隐匿在训练模型中的敏感数据；研制完成 5 种以上的敏感数据动态脱敏方式。项目执行期内新申请发明专利或软件著作权 10 项以上，发表高水平学术论文不少于 5 篇，向国内外标准化组织提交标准草案不少于 2 项。

支持方式及强度：

本专题采用竞争性评审、无偿资助方式；拟支持 2 个项目，其中项目 1 资助额度 3000 万元/项，项目 2 资助额度 1000 万元/项。

专题二：网络安全（专题编号：0137）

项目 1：大规模动态基础设施的安全管控和可信增强关键技术。

（一）研究内容

研究云计算、大数据等动态构建的信息基础设施的安全管控技术和可信计算增强技术，研究动态虚拟环境下的信息安全机制和方法，突破可信设备匿名验证、平台集群安全边界管理、平台

可生存性管理等核心技术。

（二）考核指标

项目完成时需建立面向动态和虚拟化环境的安全边界管控模型，形成模型评价体系，保证模型的可用性、可靠性、可扩展性；提出安全边界管控相关的密码学算法，支持动态和虚拟化应用环境；研制可信设备验证系统，支持匿名验证、群组验证等，验证准确率不低于 99%；研制平台集群安全边界和可生存性管理系统，支持万点规模的平台集群管理，支持群组成员的动态加入和退出。项目执行期内发表高水平研究论文不少于 5 篇，新申请发明专利或软件著作权 10 项以上。

项目 2：新型基础设施的自动网络攻防对抗关键技术。

（一）研究内容

开展攻击行为数据采集，收集目前针对主流操作系统的远程攻击代码，研究其行为特性，构建知识图谱；研究基于知识图谱的网络攻击技术和方法，实现对利用链的智能搜索及攻击框架；研究基于符号执行的系统漏洞发掘方法，主要针对主流操作系统核心部件，包括文件格式解析组件、系统调用组件等；设计基于机器学习理论的口令生成方法，替代人工产生的口令规则，根据已有的泄露口令库自动推断口令分布信息，生成爆破口令集；研究已知 shellcode 的自动利用技术和漏洞自动利用技术，完善攻击知识图谱(例如：漏洞已知但未公开攻击代码的情况)；研究基

于博弈论的最优防御策略生成及选取技术等。

（二）考核指标

项目完成时需收集近5年针对操作系统、重要软件及各大框架的远程攻击代码，要求覆盖过去5年内95%的所有有效攻击方法，构建知识图谱；开发知识图谱接口，实现基于知识图谱的攻击框架，要求在给定软件及版本的情况下给出有效的利用链及攻击代码；实现基于符号执行的漏洞挖掘工具，挖掘主流操作系统(Linux，Windows，MacOS)未知漏洞10个以上；要求样本涵盖网络上所有泄露口令，生成口令集与领英泄露口令集匹配比例高于20%；实现漏洞自动利用工具，可自动完成5个以上经典漏洞案例的攻击程序；建立基于网络系统安全测评的网络攻防博弈模型，能够对风险进行评估，并依据最优防御成本制定主动防御策略。项目执行期内发表高水平研究论文不少于5篇，新申请发明专利或软件著作权10项以上。

项目3：新型去中心化网络计算的监管和安全防护。

（一）研究内容

研究以区块链为代表的新型去中心化网络的安全防护理论体系，提出多维度、多层次、全要素可证明安全指标体系和计算模型；研究区块链安全防护架构，支持基础设施层安全、网络层安全、数据管理安全及智能合约安全；研究区块链网络中的异常行为和内容监管方法，突破区块链网络攻击等恶意行为发现和处

置、内容监测和清洗、威胁态势感知技术，研究区块链加密数字货币异常交易监测，突破用户族谱分析技术、异常账号溯源分析技术，支撑互联网金融风险分析、网络犯罪行为等应用；构建可管、可控区块链安全管控机制，研究区块链网络的防火墙和安全管控平台、并在国家有关部门开展示范应用。

（二）考核指标

项目完成时需构建不少于 10 万级节点规模、不少于 5 类区块链网络、三种业务场景下的区块链网络测试、验证环境；提出区块链网络风险评价指标体系，构建管理不少于 100 万级节点，支持对全球区块链网络的异常节点、账号、网络行为精细化评价；支持不少于 10 类异常行为的识别，识别准确度不低于 90%；构建用户族谱和交易图，支持对区块链交易图构建与攻击路线还原，支撑对区块链网络恶意行为的监测和态势感知；实现面向暗网非法交易、洗钱等跟踪监测、交易风险识别与预警、用户族谱分析以及互联网金融生态的风险识别和预警；综合项目研究成果，研制区块链网络的防火墙和安全管控平台，在国家有关部门开展示范应用，并取得实际应用效果。项目执行期内新申请发明专利或软件著作权 10 项以上，向国内外标准化组织提交标准草案不少于 2 项。

项目 4：面向边缘计算的大规模物联网安全防护关键技术与系统研究。

（一）研究内容

分析面向边缘计算的物联网安全威胁和防护需求，设计物联网安全防护体系和技术标准，解决物联网系统的多层级安全防护问题；研究物联网与其它网络系统的安全互联技术，在保证网络边界安全的前提下，解决在物联网与其它高安全等级网络之间实现高性能、高安全的数据交换问题；研究高效率、低功耗的物联网终端安全技术，包括：面向海量物联网终端的轻量级身份认证技术、高性能、高安全物联网通信协议；物联网终端安全防护技术；针对典型物联网应用场景，综合项目研究成果和关键技术，研究软/硬件相结合的综合性解决方案，开展应用示范。

（二）考核指标

项目完成时须完成典型示范应用，并产生实际应用效果；设计提出面向边缘计算的大规模物联网一体化安全防护体系；设计并研制可支持物联网安全、高速接入高安全等级网络系统的防护设备，提供网络边界防护功能；数据交换速率不低于 40Gbps；轻量级身份认证协议支持物联网终端接入数量不低于 100 万，支持双向安全认证与密钥交换；设计实现具有自主知识产权的低功耗物联网通信协议并形成技术规范；设计研制基于可信计算架构的物联网终端设备；提供从低功耗芯片、模组、终端、网关、云端服务、APP 成品一体化物联网解决方案。项目执行期内新申请发明专利或软件著作权 10 项以上，向国内外标准化组织提交标

准草案不少于 2 项。

项目 5：面向关键信息基础设施的安全评价体系及技术研究。

（一）研究内容

研究关键信息基础设施的安全管理、安全监测指标体系，打通关键信息基础设施安全管理指标与安全监测结果指标之间的关联关系，建立能够全面、客观反映关键信息基础设施安全保障水平的评价模型，研究智能化采集、分析、计算技术，并形成一套关键信息基础设施安全指数综合管理系统。

（二）考核指标

项目完成时须完成面向特定行业的关键设施基础设施安全指数综合管理系统。形成一组公开信息采集、分析与计算方法，日采集数量不小于 1 亿条；建立关键信息基础设施安全管理评价指标体系、安全监测评价指标体系并提出合理建议，评价准确度和建议的有效性均不低于 85%；建立关键信息基础设施安全管理指标与安全监测指标之间关联关系；建立关键信息基础设施安全综合评价模型；完成相关软件系统并在 3 个以上行业应用。项目执行期内新申请发明专利或软件著作权 10 项以上，向国内外标准化组织提交标准草案不少于 2 项。

支持方式及强度：

采用竞争性评审、无偿资助方式；资助额度1000万元/项。

专题三：保密技术及设备（专题编号：0138）

项目1：多路光缆安全预警设备研制。

（一）研究内容

针对机要保密单位通信光缆的信息安全要求，研发组网应用的多路通信光缆的安全预警设备。设备通过光缆感知外界针对光缆的入侵行为，分析信号，识别威胁光缆信息安全的典型事件，发出报警，并进行定位。

（二）考核指标

项目完成时须研制机要保密多路光缆安全预警设备1台，实现星形组网方式，并开展示范工程。设备须采用国产器件和模块；组网须实现一台设备不同方向不少于8条线路的安全监控，每条光缆安全检测无需占用单独光纤，只需一个波分复用信道。系统采用光路结构能够消除所监控光缆偏振态影响和光缆所处环境温度影响，偏振态稳定度大于 90%。每条光缆监控距离不小于40km（1550nm波长窗口损耗不大于10dB），对于威胁光缆的事件可以报警并定位，定位精度不少于30米。项目执行期内新申请发明专利或软件著作权20项以上。

项目2：基于自主安全SoC的高端智能彩色文印设备研制。

（一）研究内容

研究打印机核心主控SoC异构多核体系架构；研究基于国产自主指令集CPU的主控SoC软硬件文印数据操控平台；研究主控SoC内嵌安全模块；研究主控SoC内嵌DSP处理器核和硬件加速引擎单元；研究面向智能文印数据分类和优化的主控SoC内嵌NPU神经网络处理器核及应用技术；研究高端彩色激光打印成像系统并研制整机设备。

（二）考核指标

项目完成时须研制高端彩色文印设备样机1台，并形成市场应用。主控SoC芯片在40nm及以上工艺制程流片；芯片的主CPU核时钟频率达800MHz以上，性能不低于1500DMIPS；芯片内嵌国密SM2、SM3和SM4密码算法硬件单元，芯片的安全模块达到国家密码模块安全1级要求；芯片在600dpi场景下，打印处理速度不低于80PPM；整机打印速度不低于33PPM。项目执行期内新申请发明专利或软件著作权20项以上。

申报要求：

须企业牵头申报。

支持方式及强度：

采用竞争性评审、无偿资助方式；资助额度2000万元/项。

专题四：开放性课题（专题编号：0139）

（一）研究内容：

面向世界科技前沿，紧扣国家和广东产业发展需求，针对网络信息安全、国产密码技术等领域的前沿尖端技术研究、关键共性技术攻关、行业创新应用等。

（二）考核指标

鉴于网络信息安全技术领域的广泛性、研究内容的开放性以及应用场景的多样性等特点，为鼓励更多研究和应用团队围绕研究内容提出针对性的任务和目标，本专题不设具体考核指标，择优支持立论根据充足、研究目标清晰、研究内容具体、技术路线合理、应用场景明确并具备创新点的相关项目，项目总体应达到国内外一流水平。

支持强度：

本专题采用竞争性评审、无偿资助方式；资助额度根据课题研究内容和目标核算，最高不超过300万元/项。