

## **“信息安全”重大科技创新工程 2017-2018 年度项目申报指南**

为深入实施国家网络空间安全战略，提升网络安全综合实力与保障水平，有效应对未来信息安全威胁和挑战，支撑“互联网+”、网络强国战略实施，根据《山东省“十三五”科技创新规划》部署，在“十三五”期间组织实施“信息安全”重大科技创新工程，重点面向高端服务器、云计算、大数据、物联网及自动控制装备等领域的信息安全需求，研究数据、云服务、移动网络设备、工业控制系统的安全防护关键技术，研制基于可信计算体系的服务器和云数据中心，研制大数据支撑平台安全加固软件，支持信息安全产品云端转型和自主可控国产化替代，支持信息安全服务在新兴领域的应用，完善从芯片、网络、数据、应用到服务的产业链条，实现信息安全产业由大到强。

2017-2018 年度，“信息安全”重大科技创新工程重点围绕信息安全核心技术及其在云服务、大数据、移动互联网等领域的应用设置 5 个研究方向，具体内容如下：

### **1、抗量子密码算法安全关键技术**

**主要研究内容：**研究基于格的抗量子攻击的密码算法和协议的设计、分析与高效实现，研发抗量子密码实现环境及

抗量子密码支撑平台，实现多个国内外抗量子密码典型算法，设计可实用的抗量子攻击的安全协议。

**考核指标：**提出抗量子计算的密码算法并给出复杂度分析，完成实验验证；研制与抗量子密码体系相适应的 2-3 款抗量子密码产品；关键技术形成自主知识产权。

## **2、自主可控的区块链系统及其应用示范**

**主要研究内容：**围绕自主可控的区块链技术和应用，研究可扩展、高效记账、适于查询检索的区块链结构，基于国产密码技术的区块链加密机制，高效的密钥管理方案、身份识别机制、访问控制机制、共识算法，区块链合规性检测方法；研究可编程的智能合约及其底层技术，研发支持二次开发的自主可控的区块链基础支撑系统；借助云计算、并行计算等技术，开发面向不同应用的高性能区块链云管理平台，并进行应用示范。

**考核指标：**建成面向 2 个以上重点行业应用的高性能区块链应用示范系统；关键技术形成自主知识产权。

## **3、面向互联网+的云安全管控技术与系统**

**主要研究内容：**研究可定义、可重构、可演进的云服务安全防护体系；研究基于专有安全设备的主动防御技术，实现安全资源弹性扩展与按需部署；研究云数据中心内生安全机理，突破软件定义动态异构冗余、主动变迁等关键技术，实现对未知漏洞和后门威胁的主动防御；研究云服务设备的

安全态势感知、动态重构防御策略反馈，实现对安全威胁的主动和纵深防御；研究虚拟资源主动防御技术；研究云服务环境下的密码服务体系，实现密码服务系统模型构建、密码服务资源调度、敏感资源安全防护；研制包括虚拟防火墙、虚拟 VPN 网关的云安全管控系统，基于密码技术实现红黑区物理隔离和虚拟化隔离。

**考核指标：**云安全管控系统具备主流网络防御能力，其中虚拟防火墙设备转发性能达到 20Gbps，虚拟 VPN 网关加解密性能达到 1Gbps；构建云密码服务原型平台，典型应用场景不少于 5 个，密码应用安全方案通过国家密码主管部门的评审；关键技术形成自主知识产权。

#### **4、高安全等级智能移动终端的研究与开发**

**主要研究内容：**研究应用于移动智能终端的密码、证书和密钥等安全管理框架，实现加密存储、网络管理、外设管理、生物特征识别等安全增强功能；研究硬件支持的可信模式和安全隔离技术，实现可信应用的高安全隔离体系，支持多应用隔离、多用户隔离和终端虚拟化技术；研究国产密码的高安全终端密码模块实现技术，实现密码算法的运行过程安全保护和密钥保护、抵御内核级的潜在威胁，并具备可扩展性；研究终端管控策略可信实施技术，支持终端系统的高可信管控系统的实现，并能够抵御操作系统内核级的绕过、欺骗和劫持等管控对抗行为；研究面向移动智能终端的漏洞

检测与挖掘技术。

**考核目标：**至少研制一款符合主流智能终端硬件指标的产品样机，CPU 等主要部件采用我国自主研发的产品，具有操作系统和应用框架级的安全增强架构和系统化安全解决方案，支持国产密码模块，支持可信模式和终端虚拟化，实现可信安全终端管控系统；关键技术形成自主知识产权。

## **5、基于异构多源信息的安全分析、态势感知与决策关键技术**与系统

**主要研究内容：**围绕提高国家安全、政治安全为目标的大数据处理典型应用，研究多源异构信息的采集、集成和分析，研究数据聚合、自然语言理解分析、视听觉信息认知计算、网络媒体数据信任与信用评价等技术；基于数据集成分析与决策支持技术，建立实时态势感知与决策支持系统。

**考核指标：**多源信息的安全分析、态势感知与决策关键技术须支持实时安全流数据处理与实时态势感知，响应时间延迟小于 1 秒，系统部署方便、稳定可靠；在重点行业部署实施两个以上示范应用；关键技术形成自主知识产权。