附件 13

“网络空间安全”重点专项
2017 年度项目申报指南

为落实《国家中长期科学和技术发展规划纲要(2006-2020 年)》提出的任务，国家重点研发计划启动实施“网络空间安全”重点专项。根据本重点专项实施方案的部署，现发布 2017 年度项目申报指南。

本重点专项总体目标是：聚焦网络安全紧迫技术需求和重大科学问题，坚持开放发展，着力突破网络空间安全基础理论和关键技术，研发一批关键技术装备和系统，逐步推动建立起与国际同步，适应我国网络空间发展的、自主的网络空间安全保护技术体系、网络空间安全治理技术体系和网络空间测评分析技术体系。

本重点专项按照网络与系统安全防护技术研究、开放融合环境下的数据安全保护理论与关键技术研究、大规模异构网络空间中的可信管理关键技术研究、网络空间虚拟资产保护创新方法与关键技术研究、网络空间测评分析技术研究等 5 个创新链(技术方向)，共部署 47 个重点研究任务。专项实施周期为 5 年（2016-2020 年）。

2016 年，本重点专项在 4 个技术方向已启动实施 8 个研

究任务。2017 年，拟在 5 个技术方向启动 14 个研究任务，拟安排国拨经费总概算为 3.99 亿元。凡企业牵头的项目须自筹配套经费，配套经费总额与国拨经费总额比例不低于 1:1。

项目申报统一按指南二级标题(如 1.1)的研究方向进行。除特殊说明外，拟支持项目数均为 1-2 项。项目实施周期不超过 4 年。申报项目的研究内容须涵盖该二级标题下指南所列的全部考核指标。项目下设课题数原则上不超过 5 个，每个课题参研单位原则上不超过 5 个。项目设 1 名项目负责人，项目中每个课题设 1 名课题负责人。

指南中“拟支持项目数为 1-2 项”是指：在同一研究方向下，当出现申报项目评审结果前两位评价相近、技术路线明显不同的情况时，可同时支持这 2 个项目。2 个项目将采取分两个阶段支持的方式。第一阶段完成后将对 2 个项目执行情况进行评估，根据评估结果确定后续支持方式。

1.网络与系统安全防护技术研究方向

1.1 网络与系统安全体系架构研究（基础前沿类）

研究内容：针对网络大规模更新换代所面临的安全可信和管理问题，面向开放和互通的国家网络管理，研究网络和系统安全体系结构，重点研究以 IPv6 网络层的真实可信为基础的网络安全管理体系结构、关键机制和关键应用。针对未来多层次、动态、异构、差异度巨大的无线接入环境，研究新型无线网络安全接入管理机制。针对国际上新型网络与系

统体系结构的发展，如软件定义网络和系统、网络功能虚拟化、命名数据网络和系统等，对其安全问题和安全机制进行前沿探索研究。

考核指标：提出 IPv6 网络安全管理体系结构中的信任锚点、真实可信的网络定位符和标识符机制，并制定国际标准；基于上述安全可信基础，提出兼顾国际开放互通与国家安全管理的 IPv6 网络安全体系结构，通过安全威胁模型检验该体系结构的安全性。

提出 IPv6 安全管理体系结构下的关键机制，至少包括：兼顾用户隐私性、可验证性和可还原性的可信标识符认证、管理、追溯与审计机制，分级管理机制，网络监控和灵活路由机制等。

完成一套 IPv6 安全管理体系结构、关键机制和关键应用的软硬件原型系统。基于国际学术网络合作、国内主干网、园区网（校园网或企业网），对上述原理机制和原型系统进行跨国、自治系统间、自治系统内、接入子网等多层次网络的试验验证。

提出新型无线网络安全接入管理机制，研究适用在多维、异构的无线有线一体化融合网络中的信任锚点、真实可信的网络定位符和标识符机制，实现上述一体化融合网络的网络层真实可信；支持软件定义无线电，支持最新 IEEE 802.11ac 或 802.11ax 等新型无线接入技术；支持移动终端在

至少 2 种无线网络间的安全接入选择、可信透明移动。

提出 SDN/NFV 等新型组网技术和 NDN 等未来互联网体系下的安全可信问题的解决方案，提出并解决能够支持 SDN/NFV 和未来网络体系结构的可编程网络基础设施的安全问题，提出相关计算系统中的安全可信问题解决方法。

完成安全体系结构相关国际标准 3 项以上，并获国际标准组织（IETF、ITU、IEEE 等）立项或批准；申请国家发明专利 15 项以上。原理机制和原型系统需通过一定规模的真实网络试验验证，至少包括 10 个关键应用、10 万 IPv6 用户。

1.2 面向互联网+的云服务系统安全防护技术（重大共性关键技术类）

研究内容：针对体系架构、关键技术、防护系统研制等方面开展云服务系统纵深安全防护技术研究。重点研究可定义、可重构、可演进的云服务安全防护体系架构；研究分析用户和业务安全等级差异，实现高效灵活的安全服务链和安全策略按需定制；研究专有安全设备硬件解耦技术，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；实现云环境虚拟密码服务模型构建，密码服务资源动态调度，密码资源安全迁移及防护等关键技术；研究虚拟资源主动防御技术，降低侧信道攻击的风险；研究云数据中心的安全态势感知与动态重构

决策机理，实现对安全威胁的主动与纵深防御。

考核指标：建立新型云服务安全架构体系，给出适用于互联网和电信业务的安全解决方案，研制安全防护系统一套，要求：研制高性能、高可靠性的虚拟安全设备和中间件，在资源占用不超过 4 个物理 CPU 硬件线程的条件下，虚拟防火墙设备转发性能达到 30Gbps，虚拟 VPN 网关加密性能达到 2Gpbs，处理时延小于 100us，系统可靠性级别达到 5 个 9；研制安全服务编排系统，支持业务无损弹性扩展，支持亲和部署与最短路径优化。

研制云安全管理系统一套，要求：提供互联网和电信业务的 IaaS 和 PaaS 统一安全管控，支持跨数据中心和多域管理，提供安全服务开发与维护平台。

给出分布式网络控制器集群间的安全机制和南/北向安全机制等关键问题解决方案，研制抗攻击的 SDN 网络大规模集群原型系统一套，网络节点大于 10 万，租户数大于 6 万。

研制具有动态异构冗余、主动变迁等内生安全特性的用户服务系统一套，构建不少于 5 种典型攻击测试样例，搭建验证平台对控制器劫持、篡改和致瘫等安全威胁开展验证，在对外服务不间断条件下，性能降低不大于 10%，在政务、电信、金融或教育等典型云服务业务中应用，用户不少于 6 万。

建立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、敏感资源安全防护等关键技术，构建云密码服务原型平台三种典型应用场景，验证云服务中的安全增益的有效性，密码应用安全方案通过国家密码主管部门的评审。

申请国家发明专利 20 项以上；提交国际标准化草案不少于 3 项，至少 1 项获国际标准组织（IETF、ITU、IEEE 等）立项或批准。

1.3 高安全等级移动终端关键技术（重大共性关键技术类）

研究内容：面向高安全需求场景，研究高等级终端安全防护关键技术，为政务等敏感领域的移动应用推广提供技术支撑。主要研究内容包括：研究终端核心功能的高可靠安全保护技术，抵御操作系统内核级的潜在安全威胁，在终端操作系统受损的情况下，确保终端核心功能安全运行；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实现，管控实施技术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；实现基于场景识别的可信智能终端的统一管控，研究可信智能终端精确选通和智能干扰阻断技术，确保可信智能终端的接入可控、业务可管；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，在确保密码模块安全性的同时兼具可扩展性；研究终端可信用户交互

技术和可信路径；研究终端可信审计技术，实现终端系统安全事件的可信记录，能够对终端系统进行动态完整性度量。

考核指标:

研制至少 1 款产品样机，CPU 等主要部件应采用我国自主研发的产品，完成兼容现有操作系统和应用级的安全增强技术，支持利用指纹或虹膜或声纹等生物特征的系统安全增强；与现有主流智能手机相比性能下降不大于 10%，90%以上现有主流智能终端应用能直接安装使用，并实现 1000 台规模的试点应用;

安全控制核心代码量不大于 1000 行；系统信任根可控、保护链完整，附加安全核心功能至少支持加密通话和加密短信。在硬件可控和核心控制代码可信的前提下，完成整体系统安全证明，并经第三方验证。

终端应提供专门的可信状态指示器，实现终端用户与终端安全功能的可信交互，确保安全功能与用户之间的交互数据可以准确向用户展示，不被劫持、篡改。

完成高可信的终端集中管控策略实施技术，完成相关管控接口研发，通过该接口可以抵御内核级管控对抗，接口兼容相关国际标准;研制 1 套可信智能终端安全管控原型系统，具备终端检测、选通、阻断和警告功能，能防御非认证设备的伪造和重播攻击。在手机操作系统不可信的情况下，管控中心发送的管控指令能被正确执行。

实现对国产密码算法的支持，密码应用安全方案应通过国家密码主管部门评审。申请国家发明专利 20 项以上。

2.开放融合环境下的数据安全保护理论与关键技术研究

2.1 新型数据保护密码算法研究（基础前沿类）

研究内容：针对移动互联、云计算、大数据、物联网等多元化需求，以及量子攻击、白盒攻击、侧信道攻击等，开展新型密码理论和算法研究。研究新型环境下数据安全密码理论基础，重点研究新型的模块化设计理论和自动化分析理论，新型的计算复杂度分析理论和形式化验证理论；研究多方参与的数据安全计算关键密码理论，重点研究同态加密、多方认证加密、混淆密码等；研究非可信和资源受限环境下数据安全存储关键密码算法，重点研究属性加密、收敛加密、代理加密、高效可搜索加密、数据库加密等；研究随机数、密钥等密码资源受到攻击情形下的强安全数据保护密码算法，以保证灰盒攻击、白盒攻击、后门攻击等多元化攻击环境下的数据安全；研究抗量子密码算法设计理论，重点研究抗量子困难问题复杂度分析、抗量子密码算法设计理论，以满足量子计算攻击情形下的数据安全需求。

考核指标：

提出数据保护密码算法模块化设计和自动化分析的新方法。

设计多方参与的数据安全计算关键密码算法和无噪音

的同态密码算法，并完成实验验证。

设计非可信和资源受限环境下数据安全存储关键密码算法、支持多关键词和逻辑条件的密文搜索、动态密文更新的数据库外包加密，并完成实验验证。

提出在密码资源受到攻击情况下的保证密码算法安全的设计理论和技术，设计实用化的强安全密码算法。

提出抗量子计算的密码算法并给出其量子计算复杂度分析，并完成实验验证。

申请国家发明专利 20 项以上；完成国家或行业标准草案不少于 2 项，至少 1 项获得国家或行业标准主管部门立项或批准。

2.2 基于国产密码算法的移动互联网密码服务支撑基础设施关键技术（重大共性关键技术类）

研究内容：针对移动互联网的用户动态性、网络开放性以及终端设备能源、物理防护的局限性，研究密码服务支撑基础设施的服务模型和体系架构；研究面向移动互联网的密钥管理与服务关键技术，重点研究在网络不可信条件下的密钥全生命周期安全管理与服务解决方案；研究移动互联网电子认证服务技术，重点研究移动互联环境下的用户身份鉴别服务与受控使用支持技术，零延迟信任撤销技术；研究移动终端的密码计算关键技术，研发高安全的密码软件栈，研究方便易用的组件架构和应用开发框架；研究移动互联网环境

下的密码云服务技术，包括代理验证服务技术，时间戳服务技术，随机数服务技术和代理加解密技术；研究移动终端软件生态体系安全关键技术，包括移动 APP 管理密码支撑关键技术，移动 APP 版权保护技术，移动 APP 代码模块追踪溯源技术，移动 APP 代码认证签名技术；构建移动互联网密码服务示范应用，面向新型移动支付和企业移动终端安全管控需求，推进相关标准和规范的制定。

考核指标:

完成密钥管理与服务原型系统，支持网络不可信环境下的密钥生成、分发、使用、撤销与恢复；支持的移动终端数达到亿级，十万用户并发访问的非对称密钥使用服务延迟不大于 1 秒，协作式非对称密钥生成服务延迟不大于 1 秒；密钥管理与服务方案至少在半诚实模型下是可证安全的。

完成移动互联网电子认证服务原型系统，实现基于行为的、多级可信的证书签发；提供统一的在线身份鉴别服务，支持零延时的证书撤销；支持的移动终端数达到亿级规模，证书签发速度不小于 1 万张/秒，支持多种证书策略；系统应符合国家密码行业相关标准，并兼容 FIDO、SAML、OpenID、OAuth 等国际标准。

完成高安全移动终端密码软件栈，支持 10 款以上主流智能终端，对称密码算法计算效率不低于 50Mbps，数字签名算法计算效率不低于 100 次/秒；能够为智能终端管控提供

安全支撑，原型系统应当包括关键硬件资源和敏感数据的细粒度访问控制。

完成代理验证服务原型系统，支持 APP 的证书路径代理构造与验证，可支持 HTML5，支持 XML 格式交互，证书路径代理验证不大于 1 秒；完成面向移动终端的时间戳服务原型系统开发，支持 150 万次/秒的时间戳服务；完成真随机数服务原型系统开发，支持非完美移动终端密码计算的随机数需求，支持 150 万台次/秒的移动终端数字签名；完成代理加解密服务原型系统，支持移动终端与云端协作的数据加解密，对称算法加解密速率达到 50Gb/秒，支持代理重加密，加密速度 30Gb/秒。

完成移动 APP 版权保护服务系统原型及配套工具，支持移动 APP 代码认证签名，移动 APP 代码模块追踪溯源，移动 APP 安全验证。

构建移动互联网密码服务示范应用，面向新型移动支付和企业移动终端安全管控需求，推进相关标准和规范的制定，发放行业应用相关移动数字证书不少于 2 亿张。

所有系统均支持国产密码算法，密码应用安全方案通过国家密码主管部门的评审；申请国家发明专利 25 项以上；获得商用密码产品型号不少于 4 项；完成国家或行业标准草案不少于 3 项，至少 1 项获得国家或行业标准主管部门立项或批准。

2.3 互联网下的隐私保护与取证技术（重大共性关键技术类）

研究内容：主要研究数据来源隐私保护技术，包括用户时空及移动轨迹的匿名化技术，基于启发式隐私度量的位置大数据隐私保护技术，基于概率推测的位置大数据隐私保护技术；研究数据发布隐私保护技术，包括数据扰动和泛化的方法， K 匿名化和 l 多样性的方法，分布式隐私数据保护方法，数据差分隐私保护方法；研究数据计算隐私保护技术，包括支持数据关联分析的数据加密技术，支持数据多功能检索的可搜索加密技术，支持数据匿名化统计的数据加密技术；研究面向云计算的数字取证技术，包括虚拟机取证技术，面向取证的虚拟机迁移技术，虚拟身份追踪与取证技术；研究面向大数据的数字取证技术，包括基于 Hadoop 框架的大数据集群化分析技术，分布式取证分析技术，内容抽样技术；研究数据保护相关标准，包括数据安全生命周期隐私保护，含数据来源隐私保护、数据发布隐私保护和数据计算等隐私保护要求，研究大数据脱敏指南标准，研究数据分类分级安全指南标准。

考核指标：

提出互联网环境下隐私保护理论模型，提出隐私分类分级方法、隐私保护与取证需求，并与现行法律实现有效衔接。

提出互联网环境下数据来源隐私保护技术方案，并完成

技术验证原型系统开发，至少实现用户行为轨迹的匿名化和大数据环境下的用户位置信息保护等 2 种隐私保护功能。

提出互联网环境下的数据发布隐私保护技术方案，并完成验证原型系统开发，至少实现 4 种不同的数据发布隐私保护技术验证。

提出互联网环境下的数据计算隐私保护技术方案，并完成验证原型系统开发，至少实现数据关联分析、检索、和统计等 3 种操作过程中的用户隐私保护功能。

提出面向云计算和大数据环境中的取证技术方案，并完成验证原型系统开发，至少实现面向虚拟机迁移、Hadoop 等计算过程中的隐私侵犯取证技术验证。

申请国家发明专利 10 项以上；完成国家或行业标准草案不少于 5 项，至少 2 项获得国家或行业标准主管部门立项或批准。

3.大规模异构网络空间中的可信管理关键技术研究

3.1 异构身份联盟与监管基础科学问题研究（基础前沿类）

研究内容：针对网络空间中多样性网络实体的统一管理需求，研究适应多种环境的异构实体身份标识技术，防止身份信息的泄漏；针对现有身份管理技术不能支撑全面信息化环境下多形态和多域的身份安全管理的问题，研究以用户为中心的身份管理服务模式以及多形态、多域的联合身份管理技术，建立异构环境下身份联盟模型，以保证用户身份的真

实性、完整性、匿名性和可追溯性；研究多维度身份认证方法，以解决单一身份认证存在的复制和假冒问题，形成多种身份标示同在场景下的权限管理和信任管理机制，构建涵盖信任评估、信任协商等的身份动态互信任体系；针对用户身份或属性的可信度判定问题，研究适应不同场景的网络身份与属性的可信程度评价模型，实现安全属性证明及发布机制；研究异构环境中用户身份隐私保护技术，建立身份联盟行为管控模型，提出不同联盟之间用户身份资源隐私共享方法，降低用户身份信息被滥用误用的风险；研究基于网络实体身份管理的网络行为分析与监控理论，建立多态网络行为关联分析模型，研究多身份融合识别技术、行为分析技术、审计追踪技术等。

考核指标:

建立以用户为中心的面向异构网络实体身份联盟管理模型，提出多维度身份认证技术和多形态、多域的联合身份管理技术体系。建立普适性的网络实体身份标识方法，提出多类网络实体身份全生命周期管理体系。建立跨域动态权限管理模型，构建多种身份标示并存的信任管理机制，提出涵盖信任评估、信任协商等的身份动态互信任体系。建立适应不同场景的网络身份与属性的可信程度评价模型，提出多源多维度的网络身份与属性可信评价方法，并构建综合管理框架。建立具有用户隐私保护功能的身份联盟行为管控模型，

提出联盟成员之间用户身份资源隐私共享方法。提出基于网络实体身份管理的网络行为分析与监控理论体系，支持多身份融合识别、身份管理、行为分析审计等。申请国家发明专利 15 项以上。

3.2 基于国产密码算法的服务认证与证明关键技术（重大共性关键技术类）

研究内容：针对当前网络空间中由于信息服务众多，信息服务管理和验证机制缺乏，信息服务行为监管和行为可追溯能力差等现状，研究基于国产密码算法的信息服务可信管理、实体验证、可信证明、行为监管及追溯等技术体系和标准，从体系结构层面提升信息服务的可管理性、可鉴别性、可证明性、可追溯性。主要研究内容包括：信息服务的安全分级分类机制、标识机制、测评标准、评估体系、证明机制；信息服务身份管理及验证技术体系，信息服务实体化管理体系，服务联盟体系；服务可信及功能完整性证明协议、信息源可信追溯技术、信息服务责任分析及可信判定技术；信息服务可信管理平台研制，基于国产密码算法完成平台系统开发和部署，制定并发布基于相关标准和接口，并基于分类软件可信管理模型对上线运行的信息系统和服务实施可信管理和认证，具备对其功能完整性实施证明，对其安全行为实施可信追溯和责任认定能力。

考核指标:

建立信息服务安全及可信管理模型，提出相关机制原理、安全度量方法，证明协议、形成技术规范。

提出信息服务的安全分级分类方法和可信标识机制，形成信息服务安全分级分类评估标准，实现信息服务安全分级分类评估原型系统开发，具备自动化的信息服务安全分级分类，分类结果的标准符合度不低于95%。

形成支撑信息服务实体认证与功能及行为证明的核心技术标准体系；制定包括信息服务实体化可信身份管理与服务联盟、可信标识及验证、功能及行为完整性证明、可信追溯及责任判定、数据格式及接口等标准文件。

提出服务可信及功能完整性证明技术方案，至少能够针对云存储服务和虚拟主机租用服务，完成服务属性证明，包括物理位置、完整性、机密性等属性，并完成原型系统。

研制信息服务可信管理平台，基于国产密码算法，采用开放技术完成平台研制并部署，能对信息服务和系统实施可信标识，实现信息服务可信身份验证和功能及行为完整性证明，支持对信息服务实施可信追溯和责任判定。密码应用安全方案通过国家密码主管部门评审。

申请国家发明专利 10 项以上；完成国家或行业标准草案不少于5项，至少2项获得国家或行业标准主管部门立项或批准。

4. 网络空间虚拟资产保护创新方法与关键技术研究

4.1 电子货币新算法与新原理研究（基础前沿类）

研究内容：针对电子货币的发行需求和安全挑战，重点研究基于密码理论的无中心和多中心的电子货币新算法与新原理。研究电子货币的基础构造理论，以及算法和协议的可证明安全模型；研究无中心的电子货币新算法，包括电子货币共识机制、电子货币高效和匿名流通支付模型等；研究多中心的电子货币新算法，包括电子货币安全的分级发行方法、电子货币流通的授权可追踪方法与认证方法等；研究电子货币安全账本模型，包括可防伪可验证的加密账本原理等；研究电子货币安全分析模型，包括电子货币算法攻击分析和防护方法、安全能力测试和评估机制、业务风险分析及安全监管机制等。

考核指标：

提出基于密码理论的可证明安全的电子货币新算法，至少包括无中心和多中心的两类货币算法。

无中心电子货币算法在亿级用户规模下全网账本同步时间小于 10 分钟，多中心电子货币算法至少支持 2 种发行模式。

提出电子货币安全账本模型，实现电子账户密钥泄露的实时追踪和撤销算法。

实现无中心和多中心的电子货币原型验证系统。

无中心和多中心的电子货币算法至少各有一种通过国家密码主管部门的评审。申请国家发明专利 10 项以上。

4.2 安全支付及其运行监管的关键技术（重大共性关键技术类）

研究内容：探索安全电子支付的新模式新方法，在此基础上研究基于国产密码算法电子支付安全保障体系架构，重点关注移动支付中的安全需求和安全机制；研究基于国产密码的安全支付共性关键技术，包括支付服务密码基础设施、支付终端密码支持技术、密钥全生命周期统一管理、安全支付协议等；研究基于国产密码的安全支付公共系统核心技术，包括支付服务技术架构、支付服务接入金融系统的安全机制、支付数据通信安全机制、支付终端应用安全保护机制等；研究安全支付管理与行业监管关键技术，包括支付风险控制、支付过程追溯、支付系统审计与取证、系统安全性评估及系统攻击监测溯源等关键技术。

考核指标：

提出安全电子支付体系架构研究报告、电子支付国产密码应用研究报告、安全支付监管技术体系及评估方法研究报告各 1 份。编制安全支付协议规范、密码应用技术要求等国家或行业的配套标准（草案），不少于 2 份。

研发电子支付国产密码服务原型系统，支持的用户数量不小于 5 亿，带数字签名的交易支付能力达到 10 万次/秒。

研发基于国产密码的安全电子支付服务原型系统，安全电子支付终端应用，构建安全电子支付服务实验体系，并在至少 2 家电子支付服务机构投入试运行，至少与 10 家以上商业银行无缝连接，电子支付年发生笔数不小于 2 亿笔。

研发构建多维度安全支付业务风险控制模型，满足风险识别、风险评估、风险管理等安全支付管理和监管需求，风险度量方法对不同功能形态支付产品、不同平台主要支付方式具有广泛的适用性。构建分布式跨平台安全支付管理和监管原型系统，实现对跨平台支付数据安全情况的监测，实现对违规支付、异常支付、系统高风险情况的识别和管理，实现对恶意攻击的态势分析和追踪溯源等功能。

关键技术采用国产密码算法，密码应用安全方案通过国家密码主管部门的评审。

申请国家发明专利 10 项以上；完成国家或行业标准草案不少于 2 项，至少 1 项获得国家或行业标准主管部门立项或批准。

4.3 安全电子凭据服务及其监管关键技术（重大共性关键技术类）

研究内容：面向互联网电子交易、财务稽核、企业信息化等关键应用，研究适用于互联网+环境、多角色协同、高效的电子凭据安全服务体系框架及电子凭据服务监管系统与关键技术，包括电子凭据在线核准系统，电子凭据服务管

理，电子凭据相关标准规范；研究大规模用户环境下的电子凭据服务系统及关键技术，包括基于电子签名法框架的安全电子凭据协同生成、开具、查询、验证、存储与归档技术，以及公开验证技术；研究电子凭据的安全承载与应用技术，包括电子凭据离线承载，电子凭据安全存储、传输和使用，与现有应用系统、财务系统的深度融合及在线/离线审计与稽查；研究电子凭据体系运行第三方监管技术，包括互联网违规和仿冒电子凭据发行系统监测，电子凭据安全使用情况在线监测，电子凭据系统安全事件告警及追踪溯源技术等；研究基于国产密码算法的电子凭据密码支撑系统及关键技术，包括加密与认证技术，高速签名与验签技术。

考核指标:

实现一套电子凭据服务原型系统，支持多种用户鉴别方式，支持电子凭据自动和手动备份与归档，支持大存储量下的大规模并发访问，当电子凭据存储量达 100 亿张，并发访问数为 1000 时，单张凭据查询请求的响应时间小于 2 秒，验证请求的响应时间小于 1 秒。

完成电子凭据安全服务体系框架方案，实现电子凭据服务监管系统，支持细粒度监管，支持对不少于 5 个电子凭据服务系统的统一管理，电子凭据在线核准处理能力不低于 400 万张/秒。

形成适合人眼阅读和快速机读的电子凭据安全纸质承

载方案，研制至少 1 款安全的电子凭据承载传输设备与 1 套打印系统。

研发至少支持 3 款主流智能手机的移动智能终端电子凭据应用软件，支持电子凭据读取、识别、安全存储与传输。

完成电子凭据在不少于 10 款应用系统或财务系统的融合与应用，实现原型系统，支持电子凭据从开具、进入业务/财务系统到归档的全程电子化应用，支持电子凭据应用状态跟踪与控制，支持在线与离线审计的电子凭据审计和稽查。

实现电子凭据体系运行第三方监管原型系统，能够对电子凭据应用安全情况、电子凭据在线行为等方面进行监测、追溯、告警和应急处置。

实现电子凭据体系密码支撑原型系统，提供凭据签署服务速度不低于 500 万次/秒，凭据验证服务速度不低于 200 万次/秒。

密码应用安全方案通过国家密码主管部门的评审；完成电子凭据安全服务体系试点应用，应覆盖至少 10 个省或直辖市，用户数量达到 15 万人，电子凭据流转达到 700 万张/年；申请国家发明专利 10 项以上。

5. 网络空间测评分析关键技术研究

5.1 社会工程学在网络安全中的应用方法与理论研究（基础前沿类）

研究内容：针对各行业中由社会工程学带来的日趋严重

的安全问题，对社会工程学在网络安全中的应用进行原理性分析，建立社会工程学安全框架和模型，提出防御方法。研究网络安全中社会工程学理论体系，研究社会工程学、运维脆弱性和网络安全的关系，建立基于多学科交叉的社会工程学安全体系结构。研究社会工程学原理及技术，研究社会工程学中目标决策、信息收集、漏洞分析、渗透与后渗透利用方法，研究社会工程学与传统安全技术的交互、渗透、结合方法，建立社会工程学模型，为社会工程学防御奠定基础。分析社会工程学中海量社工信息的关联汇聚方法、网络空间虚拟人属性信息向物理空间自然人属性信息映射方法、网络行为信息刻画方法，构建社会工程学社工信息关联汇聚模型，研究针对性的社工信息保护方法。研究基于网络数据的社会工程学分析检测方法，研究社会工程学表示特征，提取社会工程学复杂行为模式，建立社会工程学检测模型；研究面向群体的行为模式分析方法和异常行为人检测模型构建方法，对社会工程学安全行为特征进行收集和分析，以识别攻击者并进行防护。研究运维脆弱性原理及发现技术，评估运维脆弱性带来的风险，研究针对运维脆弱性的防护方法。研究构建社会工程学行为方法库、社工信息库和人物画像库的方法，通过模拟数据和真实流量结合的方法，实现社会工程学在网络安全中应用方法的理论仿真与验证。

考核指标:

提出网络安全中社会工程学框架及社会工程学的安全理论体系，建立社会工程学攻击模型。

构建社工信息关联汇聚模型，提出针对社会工程学的社工信息保护方法，以及利用社会工程学的行为识别和防护方法。

提取社会工程学复杂行为模式，提出面向群体的行为模式分析方法，提出异常行为人检测模型构建方法，建立社会工程学行为检测模型。

构建社会工程信息描述、收集、关联体系模型，具备每天收集 2000 万条信息的能力，查全率不低于 50%，查准率不低于 50%，支持千亿级规模信息的关联聚合，支持十亿级规模人物画像库的构建。

出版学术专著 1 部；申请国家发明专利 10 项以上。

5.2 软件与系统漏洞分析与发现技术（重大共性关键技术类）

研究内容：针对漏洞分析依赖人工、缺乏有效分析工具的问题，研究典型漏洞特征分析、异常路径构造与检测等方法，面向通用计算机、移动智能终端、工业控制系统等不同计算环境，研发系列漏洞发现技术与系统，提高对不同计算平台软件与系统漏洞的发现能力与发现效率；针对软件与系统漏洞机理分析中的漏洞异常点识别、关联输入数据确定、

关键指令序列提取等问题，研究面向软件漏洞分析的数据流分析、路径约束分析、面向攻击流量的漏洞机理分析等分析方法，研发系列系统与平台，提高漏洞分析过程中对关键要素的快速分析提取能力；针对漏洞危害性评估难题，对漏洞可能造成的潜在危害进行分析，分析漏洞的利用机理，研究漏洞利用路径自动构造方法和可利用性评估方法，研发漏洞危害性评估系统，从而提高对漏洞的快速利用验证和危害性评估能力；针对漏洞发现、漏洞机理分析、漏洞危害性评估等各个环节的技术需求，研究规模化团队协同的漏洞分析与挖掘技术，研发、集成形成一套漏洞分析一体化平台，实现各环节接口的统一和部分功能的联动，以提高软件漏洞分析效率和发现能力。

考核指标:

提出的方法支持针对文本编辑、图像编辑、浏览器、安防软件等对象中的堆溢出、整型溢出、除零、空指针引用等漏洞发掘；支持针对 Windows、Linux、Android、IOS 操作系统内核和浏览器等的漏洞发掘与分析；构造软件组件级安全缺陷库，支持不少于 10 万级别的软件组件和框架，包含不少于 20 万的代码级安全缺陷信息。

软件漏洞数据流分析支持正向数据传播分析和逆向回溯分析，支持对浮点运算、多媒体处理等专用指令的分析，单条执行路径数据流平均分析效率不低于 10 万条指令/秒；

具备对局部代码模块的异常路径构造能力，路径构造可根据软件执行过程动态调整构造策略，优化路径构造效率；能够支持跨函数的代码分析，至少包含 5 种函数间分析方法。

具备漏洞异常点提取、输入数据关联等漏洞要素信息自动提取能力，可辅助用户快速确定漏洞机理，评估漏洞危害；对控制流劫持等类型漏洞可自动评估漏洞可利用性，并可对典型漏洞自动构造漏洞利用样本。

实现规模化的协同漏洞发掘平台，支持上万个节点同时工作，可支持大规模、分工合作的定向深度挖掘；百万数量软件中同源性漏洞分析达分钟级；支持对主流 PC 平台、移动终端平台、工业控制平台的软件漏洞发现和分析，漏洞发掘与分析平台支持 Windows、Linux、Android 等系统。

支持对 office、pdf 解析器、浏览器、web 组件等软件漏洞攻击样本进行自动化检测；支持不低于 1 亿样本/天的检测能力，支持 100 万对 IP/小时，其中单对 IP 流量 20pps 的检测能力；漏洞攻击样本检出误报率不高于 50%，针对测试集的检出漏报率不高于 20%；每天检出的有效漏洞利用攻击行为不低于 10 万次，其中 office、pdf 解析器和浏览器漏洞利用攻击样本不低于 1000 个。

项目周期内利用项目成果发现各类未知高危漏洞 200 个以上，并收录在 CVE 或 CNVD 或 CNNVD 等权威漏洞库中；申请国家发明专利 10 项以上。

5.3 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（重大共性关键技术类）

研究内容：面向国家网络安全态势感知和信息共享工作需求，围绕重点行业的网络安全监测、预警、应急响应和处置工作，研究适应于多元异构数据环境的数据汇聚、数据存储与管理、多元数据融合等关键技术，研发多元异构数据汇聚融合原型系统，研制数据汇聚、共享等方面的国家或行业标准；研究多类型网络安全威胁数据统计建模、多元安全事件关联分析等关键技术，面向流量、域名、报文和恶意代码的多层次异常行为，突破基于智能学习方法的未知网络攻击发现技术，研发多类型网络安全威胁数据统计分析原型系统；研究网络安全威胁识别分析、大数据可视化分析、安全决策基线建模等关键技术，研制态势感知与决策支撑原型系统，建立决策知识库；研究网络安全预警机制与持续监督方法，研制网络安全预警及持续诊断原型系统，制定网络安全风险模型与事件通报模板。

考核指标：研制 1 套多元异构数据汇聚融合原型系统，实现重点行业、企业及研究机构的网络安全资源与相关信息汇聚融合，具备 PB 量级数据的接入、存储、共享能力。研制 1 套多类型网络安全威胁数据统计分析原型系统，支持拒绝服务攻击、木马僵尸网络、恶意代码、网站后门、网页篡改、域名劫持、蠕虫利用、漏洞利用等攻击数据类型的统计

和关联分析，亿级别数据量的统计分析响应速度低于 30 秒，具备对未知攻击的感知发现能力。研制 1 套态势感知与决策支撑原型系统，同时支持 10 个以上安全事件场景的动态展示，提供态势要素信息提取功能，具备威胁识别、安全事件交互式分析和关联展示能力。研制 1 套网络安全预警及持续诊断原型系统，支持多操作系统平台，具备网络化、自动化交付能力，支持安全事件全生命周期的持续监控、处置、跟踪等。制定 1 套网络安全风险模型与安全事件通报模板，包括风险控制、防护建议、应急预案等内容。