

项目编号：2018YFB0803400

密 级：公开

国家重点研发计划 项目任务书

项目名称：	物联网与智慧城市安全保障关键技术研究
所属专项：	网络空间安全
指南方向：	1.1 物联网与智慧城市安全保障关键技术研究（共性关键技术类）
推荐单位：	中国科学院
专业机构：	工业和信息化部产业发展促进中心
项目牵头承担单位：	中国科学技术大学 (公章)
项目负责人：	李向阳
执行期限：	2018年07月 至 2022年06月

中华人民共和国科学技术部

2018年08月14日

0002YF 2018YFB0803400 2018-08-14 15:45:32



填 写 说 明

一、任务书甲方即专业机构（项目管理方），乙方即项目牵头承担单位（项目承担方）。

二、任务书通过“国家科技计划管理信息系统公共服务平台”，按照系统提示在线填写。

三、任务书中的单位名称，请按规范全称填写，并与单位公章一致。

四、任务书要求提供乙方与所有参加单位的合作协议，需对原件进行扫描后在线提交。

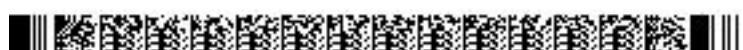
五、任务书中文字须用宋体小四号字填写。

六、凡不填写内容的栏目，请用“无”表示。

七、乙方完成任务书的在线填写，提交甲方审核确认后，用A4纸在线打印、装订、签章。一式六份报专业机构签章，其中专业机构留存三份，项目推荐单位、项目牵头承担单位和项目负责人各一份。

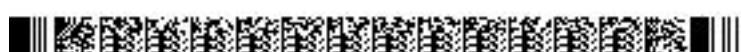
八、涉密项目请在“国家科技计划管理信息系统公共服务平台”下载任务书的电子版模板，按保密要求离线填写、报送。

九、《项目申报书》是本任务书填报的重要依据，任务书填报不得降低考核指标，不得自行对主要研究内容作大的调整。《项目申报书》和本任务书将共同作为项目过程管理、验收和监督评估的重要依据。

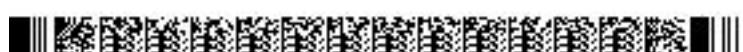


项目基本信息表

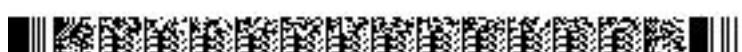
项目名称	物联网与智慧城市安全保障关键技术研究					
项目编号	2018YFB0803400					
所属专项	网络空间安全					
指南方向	1.1 物联网与智慧城市安全保障关键技术研究（共性关键技术类）					
密级	<input checked="" type="checkbox"/> 公开 <input type="checkbox"/> 秘密 <input type="checkbox"/> 机密	单位总数	21	课题数	5	
项目类型	<input type="checkbox"/> 基础前沿 <input checked="" type="checkbox"/> 重大共性关键技术 <input type="checkbox"/> 应用示范研究 <input type="checkbox"/> 其他					
	<input type="checkbox"/> 青年项目					
经费预算	总需求 2180.00 万元，其中中央财政专项经费需求 2180.00 万元					
项目周期节点	起始时间	2018 年 07 月	结束时间	2022 年 06 月		
	实施周期	共 48 个月	预计中期时间点	2020 年 06 月		
项目牵头承担单位	单位名称	中国科学技术大学		单位性质	大专院校	
	单位所在地	安徽省 合肥市 蜀山区		组织机构代码	12100000485001086E	
	通信地址	安徽省合肥市金寨路 96 号		邮政编码	230026	
	银行账号	184203468850		法定代表人姓名	包信和	
	单位开户名称	中国科学技术大学				
	开户银行(全称)	中国银行股份有限公司合肥南城支行				
推荐单位	单位名称	中国科学院	推荐单位性质	<input checked="" type="checkbox"/> 部门 <input type="checkbox"/> 地方 <input type="checkbox"/> 行业协会 <input type="checkbox"/> 产业技术创新战略联盟 <input type="checkbox"/> 其他		
项目负责人	姓名	李向阳	性 别	<input checked="" type="checkbox"/> 男 <input type="checkbox"/> 女	出生日期	1971-10-28
	证件类型	身份证件	证件号码	321025197110282833		
	所在单位	中国科学技术大学				



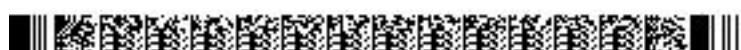
	最高学位	<input checked="" type="checkbox"/> 博士 <input type="checkbox"/> 硕士 <input type="checkbox"/> 学士 <input type="checkbox"/> 其他				
	职 称	<input checked="" type="checkbox"/> 正高级 <input type="checkbox"/> 副高级 <input type="checkbox"/> 中级 <input type="checkbox"/> 初级 <input type="checkbox"/> 其他			职务	院长
	电子邮箱	xiangyangli@ustc.edu.cn		移动电话	15152638982	
项目联系人	姓 名	吴成宝	电子邮箱	chengbwu@ustc.edu.cn		
	固定电话	0551-63607895	移动电话	13085058990		
	证件类型	身份证	证件号码	342622198506067278		
项目财务负责人	姓 名	章晨	电子邮箱	zhangchen@ustc.edu.cn		
	固定电话	0551-63606413	移动电话	13500506053		
	证件类型	身份证	证件号码	342521196210150055		
项目任务(课题)分解	序号	任务(课题)名称	任务(课题) 承担单位	任务(课题) 负责人	任务总经 费(万元)	其中中央财政 专项经费 (万元)
	01	适应智慧城市与物联网安全目标的安全架构和应用示范	中国科学技术大学	李向阳	600.00	600.00
	02	无安全代理的大规模设备智能发现、感知和监控	中国科学院信息工程研究所	姜建国	384.00	384.00
	03	基于异构标识的安全物联网互联互通机制与协议	南京邮电大学	肖甫	416.00	416.00
	04	大连接复杂异构条件下的物联网一体化安全机制	东南大学	杨明	384.00	384.00
	05	动态跨域的大规模分布式信任服务机理	清华大学	徐恪	396.00	396.00
其他参与单位	序号	单位名称		单位性质	组织机构代码	
	1	中国科学技术大学		大专院校	121000004850010 86E	
	2	中国科学院信息工程研究所		事业型研究单位	121000007178307 06J	
	3	南京邮电大学		大专院校	123200004260908 590	



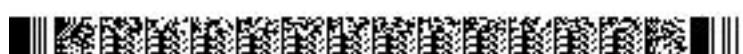
	4	东南大学	大专院校	121000004660067 70Q
	5	清华大学	大专院校	121000004000006 24D
	6	北京奇安信科技有限公司	私营企业	911101053976250 67T
	7	中移物联网有限公司	国有企业	915001080542963 889
	8	国家信息中心	事业型研究单位	121000000000180 32A
	9	北京泰豪智能工程有限公司	其他企业	911103026336518 153
	10	北京交通大学	大专院校	121000004008820 9X1
	11	北京富邦智慧物联科技有限公司	私营企业	91110108MA002GB 602
	12	太原理工大学	大专院校	121400004057000 21K
	13	合肥工业大学	大专院校	121000004000169 84P
	14	北京科技大学	大专院校	121000004000022 245
	15	中国科学院计算机网络信息中心	事业型研究单位	121000004008840 52P
	16	北京大学	大专院校	121000004000022 59P
	17	西南大学	大专院校	121000004504017 33W
	18	上海汉邦京泰数码技术有限公司	私营企业	913101107345651 66W
	19	上海交通大学	大专院校	121000004250061 5X0
	20	中兴通讯股份有限公司	国有企业	914403002793987 3X7
	21	北京理工大学	大专院校	121000004000091 27B
项目参 加人数	<u>219</u> 人。其中：		高级职称 <u>49</u> 人，中级职称 <u>27</u> 人，初级职称 <u>0</u> 人，其他 <u>143</u> 人； 博士学位 <u>51</u> 人，硕士学位 <u>37</u> 人，学士学位 <u>131</u> 人，其他 <u>0</u> 人。	
项目 简介	物联网已成为智慧城市、智慧小区等关系国计民生应用领域的关键组成部分。近年来物联网重大安全事件激增，物联网与智慧城市安全面临严重威胁，引起世界			



(限 1500 字以 内)	<p>各国普遍关注。本项目面向物联网节点计算能力、体积、功耗等限制，大规模泛在异构连接和复杂跨域的智慧城市应用需求，构建绿色、智能、开放的安全体系架构，实现物联网安全防护和管控。</p> <p>当前物联网和智慧城市安全亟需关注并解决如下三个关键科学问题：(1) 资源受限的智能感知标识；(2) 大规模泛在网络的安全异质互联；(3) 复杂跨域环境下的信任机理。</p> <p>研究内容和技术路线：</p> <p>为此，结合指南任务，项目主要围绕“三个体系架构，四项关键技术，一个原型平台和三类典型应用示范”展开研究，具体内容包括：</p> <ol style="list-style-type: none"> 1) 研究支持泛在物联网设备、异构数据的基于标识的安全物联网互联互通架构；绿色、智能、开放的物联网安全体系架构；智慧城市安全保障技术架构。研制安全物联网原型平台和支持智慧城市统一管理和隐私保护的智慧小区原型系统。 2) 研究大规模设备监控技术，实现在无安全代理条件下设备自动发现、识别及状态、行为智能感知，研制安全监管子平台，支持 10 亿规模设备发现、识别和监控。 3) 研究多物联网管理域之间的受控互联互通机制与安全协议，基于异构标识的安全物联网互联互通机制与协议。 4) 在物联网大连接、异构数据、时延复杂条件下，研究与物联网节点融合的“感存算”一体化安全机制。 5) 针对物联网跨域服务信任问题，研究基于分布式共识的大规模跨域信任服务机理及关键技术。 <p>研究基础和团队：</p> <p>项目由中国科学技术大学、中国科学院信息工程研究所、南京邮电大学、东南大学、清华大学等二十一家单位共同承担。项目组在物联网与智慧城市安全保障关键技术方面具有长期积累，获国家级奖励七项，省部级以上奖励十五项，四十多项国家发明专利。项目组承担完成了十余项国家 973/863 科研项目，为项目理论研究和技术突破提供了坚实基础。合作企业均具备良好的验证和示范环境。在物联网安全体系架构和智慧城市方面，团队拥有工业物联网软硬件开发测试平台；建成全球最大物联网专用核心网络；北京泰豪承接北京城市副中心智慧城市顶层设计、湘潭新型智慧城市等项目。在大规模设备监控方面，信工所研发物联网在线设备发现识别系统，含 4000 多种设备指纹库，在全球互联网发现 683 万监控设备和 14 万工控设备；研制“鹰眼”监控系统深度检查工具等应用于国家重要部门。同时，长期致力密码安全研究与应用，成功破解 MD5 和 SHA-1 两大密码算法，刷新多个主流物联网轻量级密码算法（PRESENT、CLEFIA、HIGHT）安全边界。</p> <p>研究目标和项目预期效益：</p> <p>项目面向大规模、异构、能力受限的物联网节点，提出数据驱动、云端结合的分级分层跨域安全体系架构；基于软件定义安全域边界，支持需求和节点资源灵活适配，实现动态跨域和自适应安全机制。实现基于身份、角色的授权策略及安全上下文敏感的动态授权管理，全面提升物联网可用性，可扩展性，与安全性。面向多源异构设备，设计跨层结构下指纹智能提取、计算、聚合、存储方法。提出基于特征相似度的设备脆弱性智能推断方法，设计高效率、低干扰的层次式设备</p>
------------------------	---



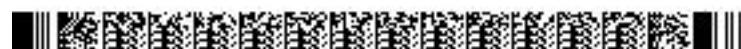
搜索方法，实现海量异构设备快速精准发现和无安全代理下安全状态智能感知。设计轻量级密钥管理方法，实现身份认证和隐私保护安全机制。面向国家新型智慧城市建设需求，将项目研制的：基于标识的安全物联网互联互通架构；绿色、智能、开放的物联网安全体系架构；智慧城市安全保障总体技术架构及关键技术，应用在智慧城市统一管理的智慧小区或智慧家庭等领域，并进行应用部署。相较于现有行业系统，有效实现连接设备超过 100 万台，接入家庭超过 20 万户，社区超过 1000 个，为实现基于物联网的智能化、柔性化、开放的城市管理提供应用示范和共性关键技术。



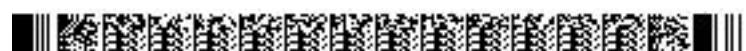
一、项目目标及考核指标、评测方式/方法

表 1：项目目标、成果与考核指标表

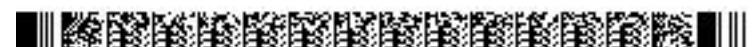
项目目标 ¹	成果名称	成果类型	对应的课题(任务) ²	考核指标 ³				考核方式(方法)及评价手段 ⁵
				指标名称	立项时已有指标值/状态	中期指标值/状态 ⁴	完成时指标值/状态	
面向物联网节点计算能力、体积、功耗等限制，大规模泛在异构连接和复杂跨域的智慧城市应用需求，急需构建绿色、智能、开放的安全体系架构，实现物联网安全防护和管控。拟采用四项关键技术，解决以下三个关键科学问题：①资源受限的智能感知标识；②大规模泛在网络的安全异质互联；③复杂	1: 适应智慧城市与物联网安全目标的全构架和应用示范	□新理论 □新原理 □新产品 □新技术 <input checked="" type="checkbox"/> 新方法 □关键部件 □数据库 □软件 □应用解决方案 <input checked="" type="checkbox"/> 实验装置/系统 □工程工艺 □标准 <input checked="" type="checkbox"/> 专利 <input checked="" type="checkbox"/> 论文 □其他	课题 1	指标 1.1 基于标识的安全物联网互联互通架构	无	完成设计方案	1 篇学术论文	论文
				指标 1.2 物联网安全体系架构	无	完成设计方案	1 篇学术论文	论文
				指标 1.3 智慧城市安全保障技术架构	无	完成设计方案	1 篇学术论文	论文
				指标 1.4 安全物联网原型平台	无	完成设计方案	完成用于安全体系架构验证的硬件设备及软件系统的支持平台。平台至少支持 2 种国密算法、支持至少 3 安全通信协议、研发	最终提交的原型平台需要通过第三方测评



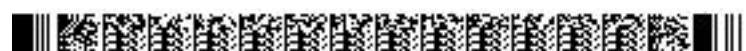
跨域环境下的信任机理。 主要研究目标：建立一体化安全关键技术，构建适应智慧城市与物联网安全目标的模型和体系框架，研制安全物联网原型平台，构建智慧小区和智慧家庭的应用示范系统。支持分级分层管理与安全解析，物联网设备发现、识别和监控以及身份认证、密钥管理服务均支持10亿规模；设计完成采用国家标准密码算法的物联网管理域的强逻辑隔离安全机制；支持基于身份和角色的授权策略映射，支持时间、环境					至少3种安全测试终端。	
			指标 1.5 智慧小区和家庭安全原型系统，开发完成支持智慧城市统一管理的安全控制中心、安全网关、智能防火墙等原型系统	无	完成设计方案	1. 防火墙吞吐量可达 240 Gbps 2. 安全网关最大并发连接数 1800 个 3. 安全控制中心的新建连接速率能力可达每秒钟 160 万个每秒
			指标 1.6 示范应用 1：智慧城市基础地理空间系统	无	完成防护体系详细设计	内网工作站具有加密和外设管理功能；内网服务器具有可信程序管理功能；具有内外网摆渡区安全防护功能；外网工作站具有外设管理功能和多模透明加密功能；外网移动工作站具有离线安全管理功能。



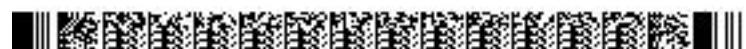
以及安全上下文敏感的授权管理，其中时间粒度不大于1分钟；开发完成支持智慧城市统一管理的安全控制中心、安全网关、智能防火墙等原型系统，并通过权威部门测评，得到试点应用；申请发明专利不少于36项，发表论文不少于38篇，其中高水平论文不少于20篇（论文是指CCF推荐A/B/C类会议或期刊，及SCI/EI期刊论文；高水平论文指CCF A/B类期刊或会议论文，及影响因子大于2.0的SCI论文），起草制定相关国际、国家或			指标1.7示范应用2：智慧城市大数据中心	无	完成防护体系详细设计	等保三级	最终提交的系统通过国家网络安全等级评估
			指标1.8示范应用3：智慧能源	无	完成防护体系详细设计	至少一个地级市示范；	最终提交的系统整体通过权威部门验收
			指标1.9示范应用4：智慧物流	无	完成防护体系详细设计	至少一个地级市示范；	最终提交的系统整体通过权威部门验收
			指标1.10示范应用5：智慧交通	无	完成防护体系详细设计	至少一个地级市示范；包含入侵检测安全技术、安全审计、防火墙、抵抗拒绝服务攻击、网络防病毒系统、流量整形和控制、加密技术和使用识别管理等功能	最终提交的系统整体通过权威部门验收
			指标1.11示范应用6：智慧城市运营管理	无	完成防护体系详细设计	至少一个地级市示范；等保三级	最终提交的系统整体通过权威部门验收；国家网络安全等级评估



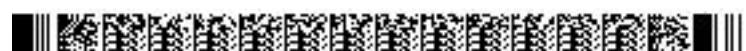
行业标准不少于3项；在2个城市实施不少于5个小区、8个典型应用的智慧小区和智慧家庭应用示范。				指标 1.12 示范应用 7：智慧教育	无	完成防护体系详细设计	至少一个地级市示范；	最终提交的系统整体通过权威部门验收
				指标 1.13 示范应用 8：智慧社区与家庭	无	完成防护体系详细设计	至少五个小区示范；具有用户隐私保护和电子支付安全防护等功能	最终提交的系统整体性能影响不超过 5%；系统整体通过权威部门验收
				指标 1.14 学术论文	无	包括上面指标中的成果，发表论文 ≥ 3 篇其中高水平论文 ≥ 2 篇	包括上面指标中的成果，发表论文 ≥ 6 篇，其中高水平论文 ≥ 4 篇	论文
				指标 1.15 发明专利	无	包括上面指标中的成果，发明专利 ≥ 5 项	包括上面指标中的成果，发明专利 ≥ 8 项	专利受理
				课题 2	指标 2.1 无安全代理的物联网设备发现技术	无	完成技术设计	实验验证 论文、专利
2：无安全代理的大规模设备智能发现、感知和监控		<input checked="" type="checkbox"/> 新理论 <input checked="" type="checkbox"/> 新原理 <input type="checkbox"/> 新产品 <input checked="" type="checkbox"/> 新技术 <input checked="" type="checkbox"/> 新方法 <input type="checkbox"/> 关键部件 <input type="checkbox"/> 数据库 <input checked="" type="checkbox"/> 软件 <input type="checkbox"/> 应用解决方案 <input type="checkbox"/> 实验装置/系统 <input type="checkbox"/> 工程工艺 <input type="checkbox"/> 标准 <input checked="" type="checkbox"/> 专利 <input checked="" type="checkbox"/> 论文 <input type="checkbox"/> 其他		指标 2.2 多维属性融合的设备识别模型及方法	无	完成技术设计	实验验证 论文、专利	
				指标 2.3 设备安全状	无	完成技术设计	实验验证 论文、专利	



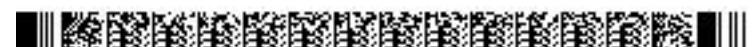
			态探测与 行为智能 推断方法				
			指标2.4物 联网安全 监控子平 台	无	支持5亿规 模的设备 发现；识别 设备的种 类≥10种， 数量支持5 亿规模；识 别准确率 不低 于 80%；支持5 亿规模的 设备安全 状态探测； 不少于3种 僵尸节点 检测能力， 数 量 不少 于6万	实现无代理 的物联网设 备发现，支持 10亿规模设 备发现；识别 设备的种类 ≥15种，包括 但不限于摄 像头、打印 机、路由器、 PLC、RTU、 SCADA、智能 开关、智能照 明、智能穿戴 等；数 量 支 持10亿规模； 识别准确率 不低于95%； 实 现 物 联 网 设备状态的 智能推断，支 持10亿规模； 不 少 于 5 种 僵 尸 网 络 物 联 网 节 点 检 测 能 力， 总 体 僵 尸 节 点 数 量 不 少 于 10 万。	第三方测评
			指标2.5学 术论文	无	包括以上 成果，论文	包括以上成 果，论文≥6	论文



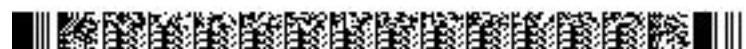
					≥ 3 篇，其中高水平论文 ≥ 1 篇	篇，其中高水平论文 ≥ 3 篇	
				指标 2.6 发明专利	无	包括以上成果，发明专利 ≥ 5 项	包括以上成果，发明专利 ≥ 8 项
	3. 基于异构标识的安全物联网互联互通机制与协议	课题 3		指标 3.1：物联网设备标识生成原型系统	无	完成设计方案	支持设备种类不少于 10 种（如 RFID 标签、二维码标签、摄像头标识等），设备标识的生成特征不少于 5 种（如标识物理状态、感知状态、安全状态等）。
				指标 3.2：与现有 zigbee 等通信协议、RPL 等路由协议的兼容架构	无	初步设计	一套实验装置，支持物联网通信协议不少于 4 种（如 NB-IOT，LoRa，蓝牙，wifi，zigbee）、路由协议不少于 4 种（AODV、LEACH、SPIN、SEIF 等）
				指标 3.3：面向异构标识的轻	无	初步设计	支持异构标识种类 3 种以上（RFID、二



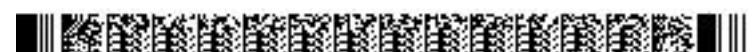
			量级域间及跨域身份认证和高效数据隐私保护机制			维码、条形码等等), 支持隐私数据类型 8 种以上(位置、时钟、属主等)	
			指标 3.4: 基于区块链、DHT 的异构标识对等跨域解析机制	无	初步设计	支持异构标识种类3种以上(RFID、二维码、条形码等等)。	标准送审稿
			指标 3.5: 提出物联网跨域多维分级授权访问控制机制与协议架构	无	初步设计	管理域数量 4(管理域一-Zigbee 无线网络协调器管理域; 管理域二-网关管理域; 管理域三-本地或远程服务器管理域; 管理域四-云存储服务管理域), 身份数量 15 (身份即节点标识, 即节点标识数量 15), 角色数量 4 (源节点角色、目的节点角色、网关管理节点角	论文或专利



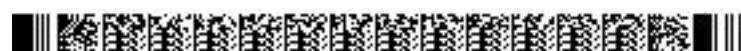
						色、云存储服务角色)	
				指标 3.6: 物联网跨域多维分级授权及访问控制方法	无	初步设计	实现多维分级授权功能验证 技术报告及专家鉴定意见
				指标 3.7: 学术论文	无	包括以上成果, 论文总数 ≥ 4 篇, 其中高水平论文 2 篇	包括以上成果, 论文总数 ≥ 8 篇, 其中高水平论文 4 篇 论文
				指标 3.8: 发明专利	无	包括以上成果, 发明专利总数 ≥ 6 项	包括以上成果, 发明专利总数 ≥ 12 项 专利受理
				指标 3.9: 标识标准	无	包括以上成果, 标准立项 ≥ 1 项	包括以上成果, 标准送审稿 ≥ 2 项 标准送审证明
4: 大连接复杂异构条件下的一体化安全机制	<input type="checkbox"/> 新理论 <input type="checkbox"/> 新原理 <input type="checkbox"/> 新产品 <input checked="" type="checkbox"/> 新技术 <input checked="" type="checkbox"/> 新方法 <input type="checkbox"/> 关键部件 <input type="checkbox"/> 数据库 <input type="checkbox"/> 软件 <input type="checkbox"/> 应用解决方案 <input type="checkbox"/> 实验装置/系统 <input type="checkbox"/> 工程工艺 <input checked="" type="checkbox"/> 标准 <input checked="" type="checkbox"/> 专利 <input checked="" type="checkbox"/> 论文 <input type="checkbox"/> 其他	课题 4	指标 4.1 异构数据的可信感知技术	无	完成情境识别感知方案设计	情境识别感知准确率 $\geq 85\%$; 虚假数据检测准确率 $\geq 90\%$	论文
			指标 4.2 基于PUF、物理指纹的异构节点认证方	无	认证节点数 ≥ 5 种	认证节点种类 ≥ 15 种, 终端节点认证的错误接受率 $\leq 10\%$	论文



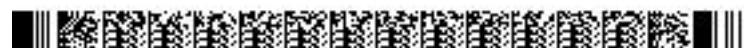
			法			错误拒绝率 ≤5%	
			指标 4.3 智 能 网 关、智能 防火墙中 的隐私保 护功能	无	完成设计 方案	数据隐私保 护针对可量 化的数据查 询，数据差 分隐私预算 ≤1，数据噪 声比≤5%或 查询结果误 差≤5%；通 信隐私保护 可抵御基于 流量分析的 侧信道攻击	论文
			指标 4.4 基 于 低 延 迟 / 轻 量 级 / 功 能 加 密 的数 据 传 输 和 存 算 机 制	无	完成设计 方案	设计解决方 案，为延迟 敏感应用提 供低延迟加 密服务，为 感知数据存 储和计算提 供相应的加 密服务	专利
			指标 4.5 学 术 论 文	无	包括上面 成果，论 文 总 数 ≥2 篇，其	包括上面成 果，论文总 数≥8 篇， 其中高水平	论文



					中高水平论文总数 ≥1篇	论文总数 ≥4篇	
				指标 4.6 发明专利	无	包括上面成果，发明专利总数 ≥2项	包括上面成果，发明专利总数 ≥4项
				指标 4.7 标准	无	无	完成标准 (送审稿)1项
							专利受理
5. 动态跨域的大规模分布式任务管理	<input checked="" type="checkbox"/> 新理论 <input type="checkbox"/> 新原理 <input type="checkbox"/> 新产品 <input type="checkbox"/> 新技术 <input checked="" type="checkbox"/> 新方法 <input type="checkbox"/> 关键部件 <input type="checkbox"/> 数据库 <input type="checkbox"/> 软件 <input type="checkbox"/> 应用解决方案 <input checked="" type="checkbox"/> 实验装置/系统 <input type="checkbox"/> 工程工艺 <input type="checkbox"/> 标准 <input checked="" type="checkbox"/> 专利 <input checked="" type="checkbox"/> 论文 <input type="checkbox"/> 其他	课题 5	<p>指标 5.1: 密钥管理服务支撑</p> <p>指标 5.2: 采用国家标准密码算法的物联网服务域的强逻辑隔离安全机制</p> <p>指标 5.3: 完成多物联网服务域之间的协作互信协议</p>	<p>无</p> <p>无</p> <p>无</p>	<p>完成设计 方案</p> <p>完成跨服务域强隔 离的详细 设计</p> <p>完成设计 方案</p>	<p>1 篇学术论文</p> <p>服务域之间 的初始状态 实现强逻辑 隔离</p> <p>完成 10 亿规 模的密钥管 理服务支撑； 完成基于身 份和基于角 色的授权策 略映射，时间 粒度应≤1 分 钟</p>	<p>论文</p> <p>通过国家主 管部门安全 审查</p> <p>最后平台完 成第三方测 评</p>

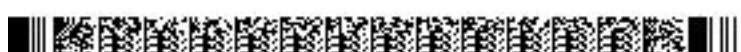


			指标 5.4 学术论文	无	包括上面成果, 论文 ≥ 5 篇, 其中高水平论文 ≥ 2 篇。	包括上面成果, 论文 ≥ 10 篇, 其中高水平论文 ≥ 5 篇。	论文
			指标 5.5 发明专利	无	国家发明专利 ≥ 1 项, 国际发明专利 ≥ 1 项	国家发明专利 ≥ 2 项, 国际发明专利 ≥ 2 项	专利受理
科技报告考核指标	序号	报告类型 ⁶	数量	提交时间		公开类别及时限 ⁷	
	1	项目年度技术报告	4	2019 年/2020 年/2021 年 12 月 2022 年 6 月		延期公开 2 年	
	2	项目中期技术报告	1	2020 年 12 月		延期公开 2 年	
	3	项目最终技术报告	1	2022 年 6 月		延期公开 2 年	
	4	课题年度技术报告	20	2019 年/2020 年/2021 年 12 月 2022 年 6 月		延期公开 2 年	
	5	课题中期技术报告	5	2020 年 12 月		延期公开 2 年	
	6	课题最终技术报告	5	2022 年 6 月		延期公开 2 年	
其他目标与考核指标 (对于难以采取上述表格细化的项目目标及其考核指标, 可在此细化填写。)							



备注：

1. “**项目目标**”，应从以下方面明确描述：(1) 项目研发主要针对什么问题和需求；(2) 将要解决哪些科学问题、突破哪些核心/共性/关键技术；(3) 预期成果；(4) 成果将以何种方式应用在哪些领域/行业/重大工程等，并拟在科技、经济、社会、环境或国防安全等方面发挥何种的作用和影响。
2. “**对应的课题（任务）**”，指将由项目内哪些课题（任务）支撑取得某项成果。
3. “**考核指标**”，指相应成果的数量指标、技术指标、质量指标、应用指标和产业化指标等，其中，数量指标可以为论文、专利、产品等的数量；技术指标可以为关键技术、产品的性能参数等；质量指标可以为产品的耐震动、高低温、无故障运行时间等；应用指标可以为成果应用的对象、范围和效果等；产业化指标可以为成果产业化的数量、经济效益等。同时，对各项考核指标需填写立项时已有的指标值/状态以及项目完成时要到达的指标值/状态。同时，考核指标也应包括支撑和服务其他重大科研、经济、社会发展、生态环境、科学普及需求等方面的直接和间接效益。如对国家重大工程、社会民生发展等提供了关键技术支撑，成果转让并带动了环境改善、实现了销售收入等。若某项成果属于开创性的成果，立项时已有指标值/状态可填写“无”，若某项成果在立项时已有指标值/状态难以界定，则可填写“/”。
4. “**中期指标**”，各专项根据管理特点，确定是否填写，阶段目标明确的专项项目应填写中期指标。
5. “**考核方式方法**”，应提出符合相关研究成果与指标的具体考核技术方法、测算方法等。
6. “**科技报告类型**”，包括项目验收前撰写的全面描述研究过程和技术内容的最终科技报告、项目年度或中期检查时撰写的描述本年度研究过程和进展的年度技术进展报告以及在项目实施过程中撰写的包含科研活动细节及基础数据的专题科技报告（如实验报告、试验报告、调研报告、技术考察报告、设计报告、测试报告等）。其中，每个项目在验收前应撰写一份最终科技报告；研究期限超过2年（含2年）的项目，应根据管理要求，每年撰写一份年度技术进展报告；每个项目可根据研究内容、期限和经费强度，撰写数量不等的专题科技报告。科技报告应按国家标准规定的格式撰写。
7. “**公开类别及时限**”，公开项目科技报告分为公开或延期公开，内容需要发表论文、申请专利、出版专著或涉及技术诀窍的，可标注为“延期公开”。需要发表论文的，延期公开时限原则上在2年（含2年）以内；需要申请专利、出版专著的，延期公开时限原则上在3年（含3年）以内；涉及技术诀窍的，延期公开时限原则上在5年（含5年）以内。涉密项目科技报告按照有关规定管理。



二、项目研究内容、研究方法及技术路线

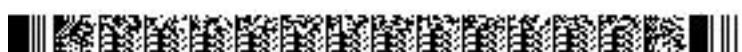
（一）项目的主要研究内容

物联网节点种类繁多、结构功能异构、计算及能量资源普遍受限。在智慧城市应用背景下，物联网存在大规模泛在异构连接、复杂跨域的特点，网络的规模和复杂度更进一步提升带来的安全挑战。然而，现有的物联网安全解决方案普遍存在代价高，普适性差，可扩展性差等缺点，无法满足大规模复杂物联网的安全需求。为了实现大规模物联网安全防护和管控，急需构建一个**绿色、智能、开放**的安全体系架构。本项目拟研究动态跨域的大规模分布式信任服务机理，大连接复杂异构条件下的物联网一体化安全机制，基于异构标识的安全物联网互联互通机制与协议以及无安全代理的大规模设备智能发现、感知和监控这四项关键技术，解决“资源受限的智能感知标识”、“大规模泛在网络的安全异质互联”、“复杂跨域环境下的信任机理”三个关键科学问题。

项目组联合 21 家优势单位，围绕指南方向和任务要求，重点研究物联网与智慧城市安全保障关键技术。项目共分为五个课题，每个课题的主要研究内容如下：

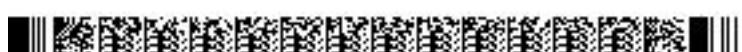
课题 1：适应智慧城市与物联网安全目标的安全架构和应用示范。研究智慧城市与安全物联网体系架构，并研制系统平台和应用示范。主要研究内容包括：①结合轻量级密钥生成、协商、分发、更新的密钥管理技术，以及应用可信认证、消息认证、跨域身份认证等认证技术，研究支持泛在物联网设备和异构数据，支持强逻辑访问控制，支持多维度授权管理，具有隐私保护能力的基于标识的安全物联网互联互通架构；②结合安全态势智能管控、应用安全管理、网络分层安全管理、设备分级安全管理等安全保障技术，并针对智慧城市的应用层、数据层、网络层、感知层特有的安全隐患设计相应解决方案，设计智慧城市安全保障技术架构；③研制安全物联网原型平台，支持大规模物联网对象分级管理与安全解析，物联网设备发现、识别和监控以及身份认证、密钥管理服务均支持 10 亿规模；④研制支持智慧城市统一管理与支持隐私保护的智慧小区和智慧家庭适用的安全控制中心、安全网关、智能防火墙等原型系统，并通过权威部门测评，得到试点应用。

课题 2：无安全代理的大规模设备智能发现、感知和监控。研究大规模设备监控技术，实现在无安全代理条件下设备自动发现、识别及状态、行为智能感知，具体研究内容包括：①结合水平搜索、垂直搜索、任务分配和资源调度等机制，研究高效率、低干扰的全球设备层次式探测策略，以及信息熵最大化的设备快速搜索方法；研究基于决策



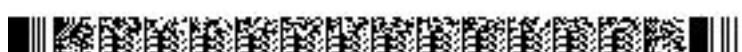
树的多指纹模型的策略优化调度方法；研究无打扰、跨网跨域、主被动结合的物联网设备搜索技术，实现无安全代理条件下设备自动发现；②结合物联网设备的多维属性，研究多维融合的设备识别模型；基于自然语言处理和机器学习方法，研究物联网设备及网络行为特征自动化提取和识别技术；③基于物联网设备远程可访问文件的安全性分析，研究能够发现多种脆弱性的主动探测方法；基于设备关联关系或漏洞信息匹配，研究信息不对称条件下的设备脆弱性模糊推断方法；研究采集数据安全感知机制；基于恶意代码的传播特性，并结合蜜罐、IP 溯源及同源行为特征，研究网络空间中的恶意物联网设备（被利用物联网设备）的主动检测方法和由恶意设备组成的僵尸网络的鉴别机制；④研发物联网设备发现子系统、识别子系统、及感知子系统，并集成为物联网安全监控子平台，支持 10 亿规模的物联网设备发现、识别和监控。

课题 3：基于异构标识的安全物联网互联互通机制与协议。研究多物联网管理域之间的受控互联互通机制与安全协议，提出基于标识的安全物联网互联互通架构，具体内容包括：①根据无线链路和路由特征，对设备进行唯一地址编码标识的生成和验证。研究基于 RFID、传感标签等及其位置信息的标识生成方法和验证；研究基于通信信道信息的标识生成方法和轻量级密钥交换方法；②研究大规模泛在网络中异构通信协议安全融合互联机制，包括多元协议泛化和异构协议映射；研究大规模泛在网络中多层跨域受控安全数据路由协议，包括域内协议耦合和跨域数据路由；③基于标识的域内轻量级身份认证，针对物联网标识认证协议缺乏严格的安全性证明问题，提出满足非对称密码算法系统要求的可证明安全的标识认证模型；基于区块链的跨域身份认证，研究基于区块链的去中心化、分布式的点对点身份认证机制；研究基于 PIN (Personal-Identification-Number 个人识别码) 标识支持口令保护的终止命令方法和基于 PIN 认证的标识支持睡眠命令的改进方法解除设备和标识之间关联性；④研究基于区块链、DHT 的异构标识对等解析互通机制，研究标识映射关系的防篡改方法，实现支持异构标识的对等解析互通架构；研究标识解析的权限保护、查询的安全、查询的权限设置、标识解析应答和映射关系的不可篡改和防止映射关系被劫持等安全机制，实现标识解析的安全机制；⑤研究大规模物联网跨域多维授权及访问控制模型。针对大规模物联网的跨域分级授权访问控制实施问题，研究大规模物联网层簇式树形授权管理结构、用户注册流程、用户分级原则、管理域分级原则、访问授权原则；针对物联网的跨域多维分级授权及访问控制模型的安全性证明问题，研究构造形式化敌手模型。



课题 4：大连接复杂异构条件下的物联网一体化安全机制。在物联网大连接、异构数据、时延复杂条件下，研究与物联网节点融合的“感传存算”一体化安全机制。①在感知阶段，综合利用多种感知数据，研究基于异构数据的可信感知机制，包括多因子情境识别感知技术和安全异构数据融合技术，实现对异构数据的可信感知，并且对感知数据源的持续安全检测，保证数据融合的安全性；②在传输阶段，研究面向大连接、时延复杂条件的安全传输机制，包括基于 PUF/物理指纹的轻量级认证技术、低延迟加密的数据传输技术、基于标识的大规模密钥管理机制和多模态流量伪装技术，实现节点的安全接入和通信隐私保护，并且可兼容计算资源、功耗受限的节点，同时也提高了实时响应速度；③在存储和计算阶段，研究面向异构数据的安全存算机制，包括基于轻量级/功能加密的数据存算机制和基于差分隐私的感知数据处理机制，实现数据的安全存储、计算和隐私保护；④研究面向物联网节点的安全和性能优化机制，包括面向大连接、时延复杂的云端融合机制和面向节点资源受限的传算结合机制，设计云端融合、传算结合的体系结构以及优化策略，完成协同任务的优化分配，实现节点资源约束下的安全和性能优化平衡。

课题 5：面向动态跨域的大规模分布式信任服务机理。针对复杂跨域环境下的信任问题，从“隔离—协作—互信—管控”四个阶段入手，研究大规模跨域信任服务机理及关键技术。①针对“隔离”阶段不同管理域之间的数据隐私保护难题，基于国家标准密码算法，研究物联网管理域之间的强逻辑隔离安全机制。②为了保障管理域“协作”时的数据完整性和可信性难题，研究跨域身份信息与认证技术。③面向管理域“互信”时的密钥管理和安全策略协商两方面难题，研究基于秘密共享的轻量级域内密钥管理机制，提高资源受限的物联网设备密钥分配响应速度；研究基于身份的无可信第三方的域间密钥管理方案，通过分布式秘密共享建立顶层管理域间的信任机制，消除对可信第三方的依赖，通过基于身份的密钥算法实现无证书的跨域密钥协商；研究复杂管理域下的安全策略协商协议，在确保协商效率的前提下有效实现对通信双方的隐私保护。④面向跨管理域“管控”时的访问控制和数据交换难题，针对跨域不兼容和跨域用户数据访问隐私性的问题，研究基于身份和基于角色的授权策略映射，支持时间、环境以及安全上下文敏感的授权管理。



(二) 项目采取的研究方法

本项目围绕三大科学问题，着力突破四项关键技术，通过设计互联互通，物联网安全和总体技术三个方面体系架构，结合一个系统平台，进而实现智慧城市的典型应用。从多维融合模糊推断、分层解析跨域认证、云端融合传算结合、动态跨域软件定义四个方面的关键技术展开研究，总体研究思路如图 2.1 所示。

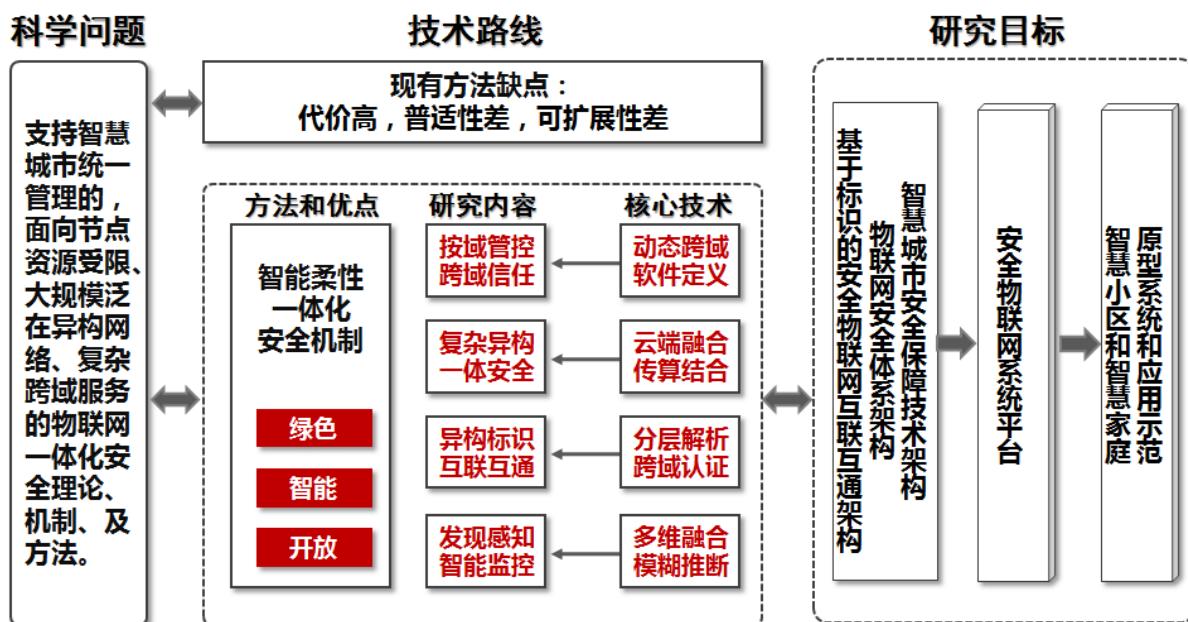


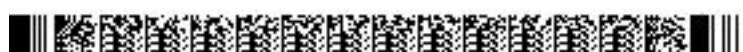
图 2.1 项目总体研究思路

本项目共设置 5 个课题，各课题拟采取的研究方法如下：

(1) 课题 1 研究方法及思路

如图 2.2 所示，首先解决共性关键技术问题，满足物联网基本安全需求。从构建面向智慧城市与物联网安全为核心目标的安全架构出发，结合共性基础安全关键技术，进一步提出数据服务层、计算存储层、网络层和感知层的关键技术。在此基础之上，构建应用示范平台，支撑物联网设备的智能发现与管理、互联互通、跨域连接、存储管理、以及具有隐私保护功能的数据服务。

其次，根据智慧城市的安全建设需求，研究智慧城市安全保障技术架构。从通用技术出发，结合智慧城市安全保障的实际需求，推动技术架构在不同行业中的应用。在技术体系方面，从安全技术体系、管理体系、运维体系三个角度出发，设计一套完整的安全保障体系，为物理与环境安全、系统安全、网络安全、及数据和应用安全设计全方位的安全保障体系。



最后，结合智慧家庭、智慧小区及智慧城市管等 8 个典型应用对安全体系架构进行验证。

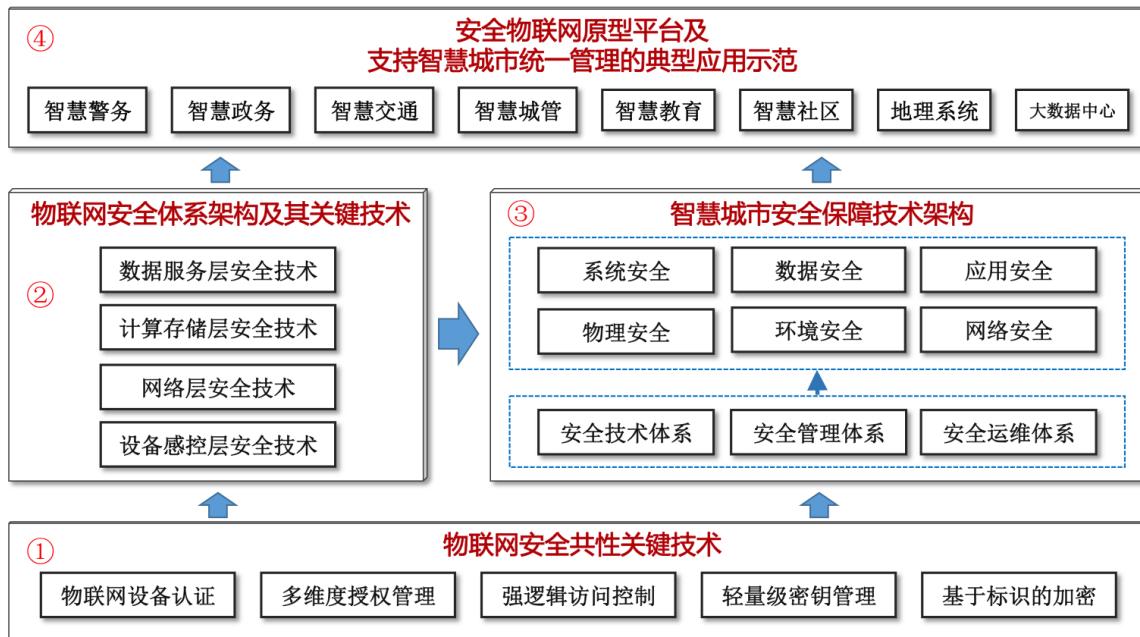
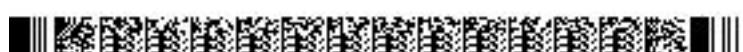


图 2.2 课题 1 拟采用的研究方法及思路



(2)课题2 研究方法及思路

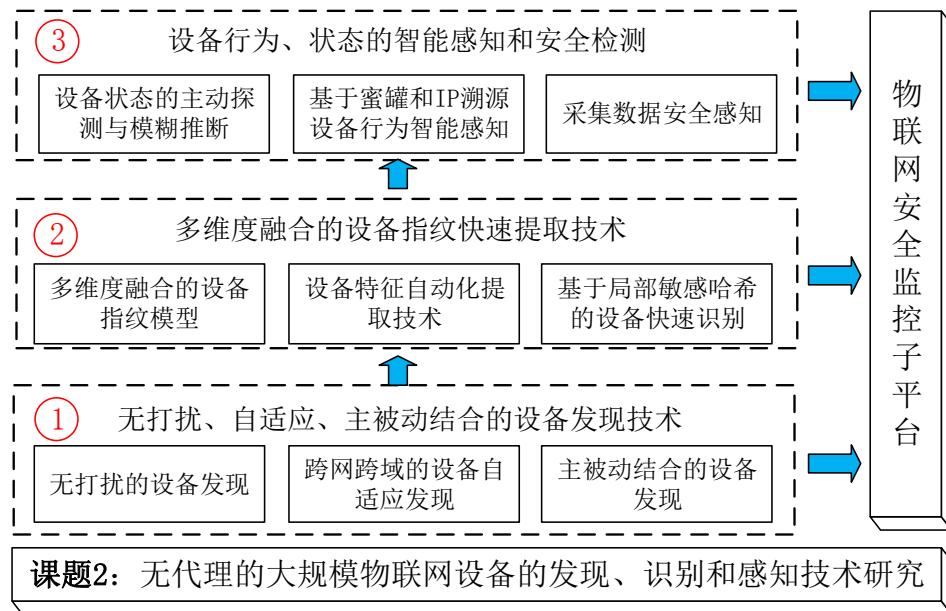
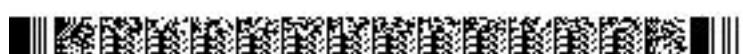
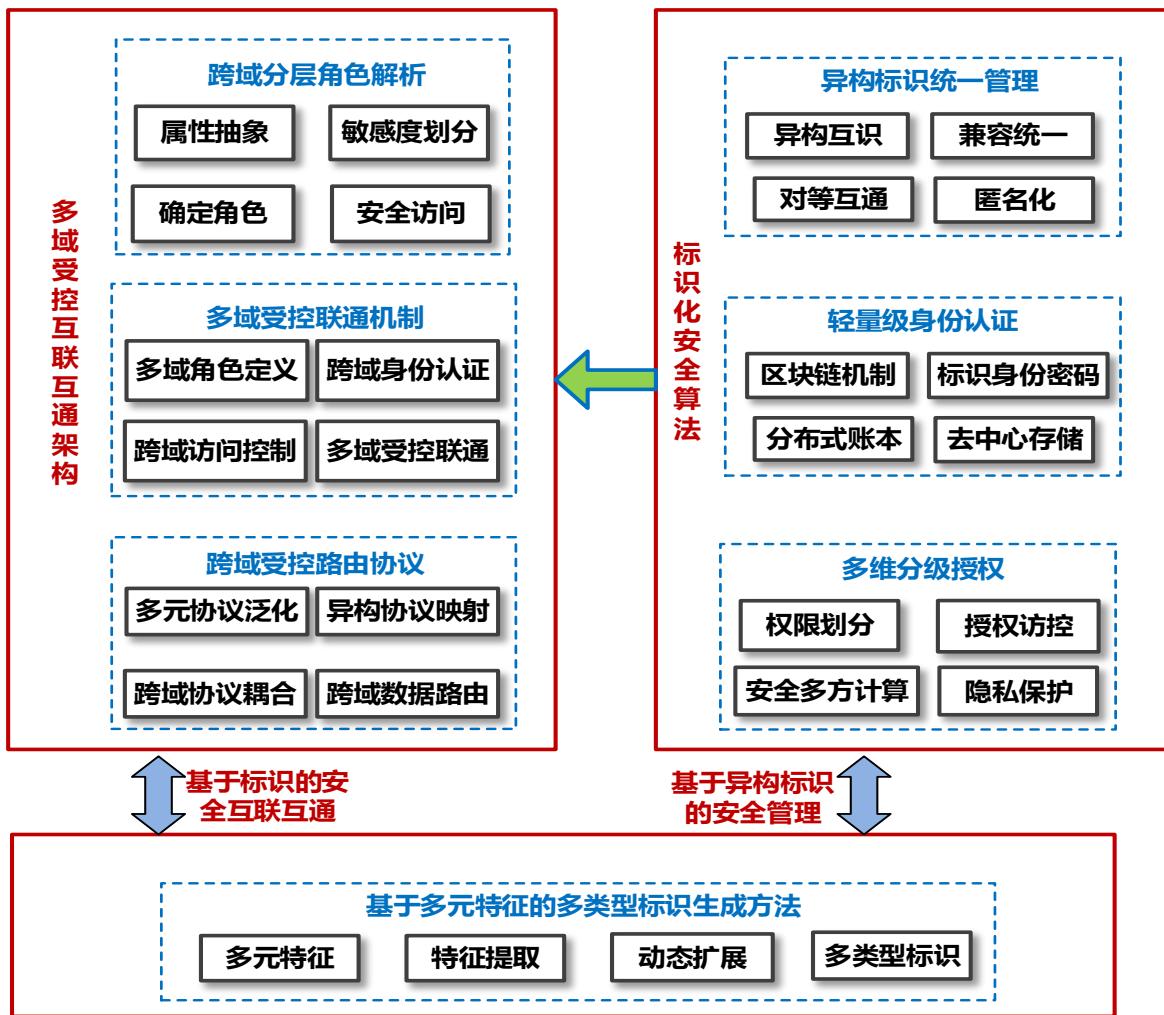


图 2.3 课题 2 拟采用的研究方法及思路

如图 2.3 所示, 步骤 1: 提出无打扰设备发现技术, 降低探测对网络空间的干扰影响; 提出跨网跨域自适应设备发现算法, 找到网络空间中异构和自组织的物理设备; 提出主动探测和被动侦听结合的设备发现技术, 扩大覆盖范围。步骤 2: 提出多维特征信息融合模型, 提高设备指纹的识别精度; 提出基于规则指纹自动生成技术, 自动识别物联网设备; 提出基于哈希值的指纹生成技术, 实时发现物理设备。步骤 3: 提出基于主动探测和模糊测试技术的状态模型, 推测设备安全状态; 提出基于蜜罐和 IP 溯源技术的行为模型, 感知物联网空间设备行为; 提出智能感知的数据安全采集技术, 保障设备感知的安全。步骤 4: 为满足无代理的大规模设备发现、识别和智能感知, 建立面向物联网安全监管子平台, 支持 10 亿规模设备发现、识别和监控。



(3)课题3 研究方法及思路



(4)课题4 研究方法及思路

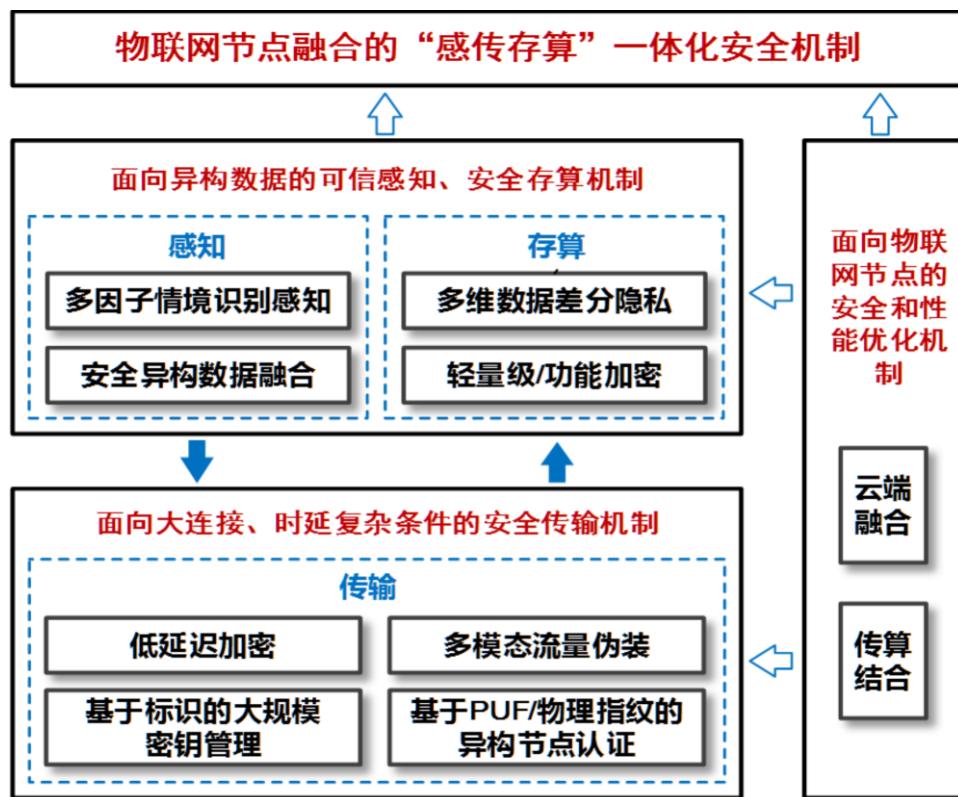
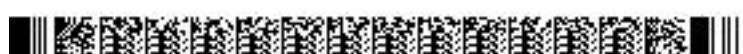


图 2.5 课题 4 拟采用的研究方法及思路

如图 2.5 所示，包括：(1) 针对物联网中数据多源异构的特点，研究多因子情境识别感知技术和安全异构数据融合技术。(2)针对大连接条件下异构节点的安全接入问题，研究基于 PUF、物理指纹的轻量级认证技术；提出基于标识的大规模密钥管理机制，以简化密钥管理；针对时延复杂特点及其带来的侧信道隐私泄露威胁，研究基于低延迟加密算法的自适应数据传输技术；基于流量变换等方法，研究自适应的多模态流量伪装技术。(3) 针对数据存算时存在的隐私泄露风险，研究基于差分隐私的用户敏感数据保护机制、基于轻量级加密的数据存储机制和基于功能加密的数据存算机制。(4) 针对大连接、时延复杂的特点，研究云端融合和传算结合机制，在延迟敏感和资源约束条件下自适应地分配安全计算任务，从而达到安全和性能优化的平衡。



(5)课题5 研究方法及思路

如图 2.6 所示，包括：(1) 在“隔离”阶段，针对不同服务域之间数据隐私的问题，基于国家标准密码算法，研究采用软件定义的方式实现服务域之间强逻辑隔离的安全机制；(2) 在“协作”阶段，针对复杂跨域环境下的协作信任问题，研究基于分布式共识理论，建立跨域身份信息与认证技术，保证跨域通信之前的身份信息与平台配置的可信性；(3) 在“互信”阶段，针对域内资源受限环境，研究轻量级密钥管理协议与算法。在此基础上，针对域间复杂服务域环境，研究基于身份的无可信第三方密钥管理，实现分布式跨域密钥协商。基于域间密钥协商实现高效的安全策略协商，实现交互双方的隐私保护。(4) 在“管控”阶段，针对跨服务域的访问控制与数据交换问题，设计基于软件定义的授权策略映射，实现分钟级粒度的授权管理，保证访问控制和数据交换的安全性。

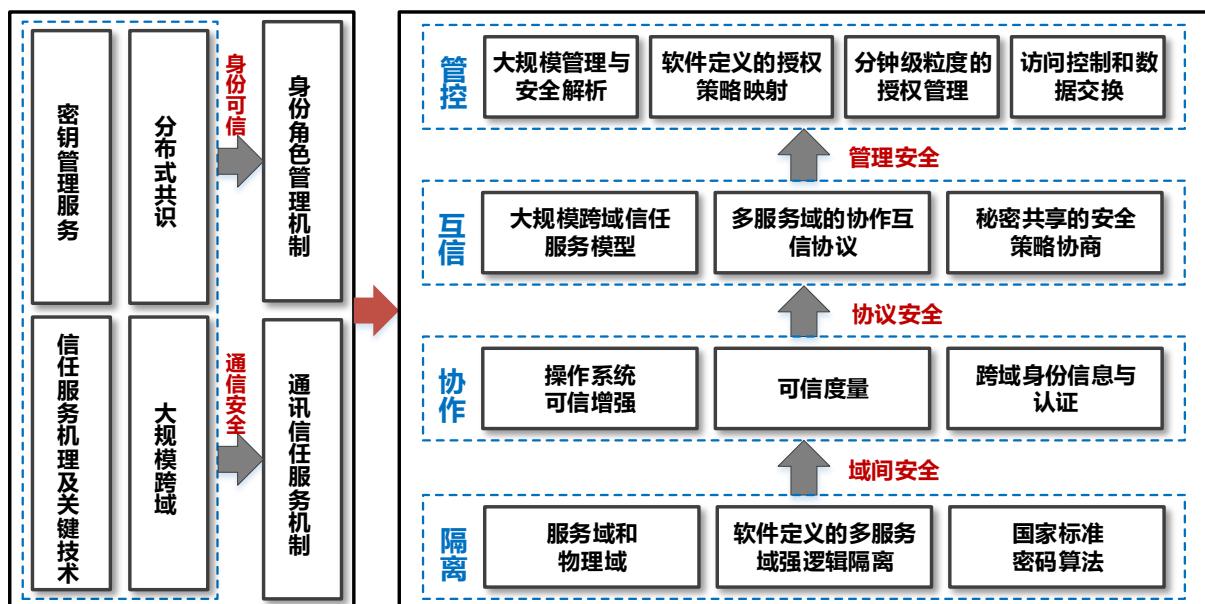
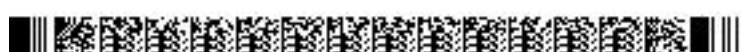


图 2.6 课题 5 拟采用的研究方法及思路



三、项目任务(课题)分解

(一) 项目任务(课题)分解情况

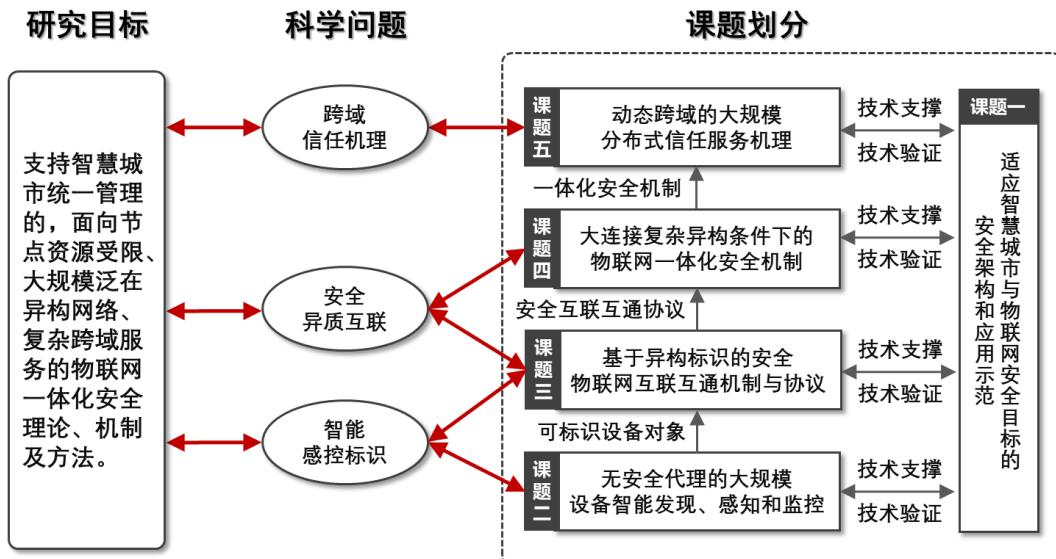


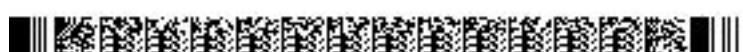
图 2.7 项目目标、课题分解及支撑情况

紧扣指南中凝练的项目总体目标：“研究建立支持智慧城市统一管理的，面向节点资源受限、大规模泛在异构网络、复杂跨域服务的物联网一体化安全理论、机制及方法”，遵照上述“研究方案”部分所阐述的学术思想、研究方法及技术路线，针对“资源受限的智能感知标识”、“大规模泛在网络的安全异质互联”、“复杂跨域环境下的信任机理”三大关键科学问题，从“基础理论-应用技术-原型系统”三个层面建立以下五个课题：

课题一：适应智慧城市与物联网安全目标的安全架构和应用示范

该课题涵盖网络安全体系架构设计和平台示范系统研制两方面内容。主旨在于建立大规模泛在物联网的安全体系架构、研制安全物联网原型平台，并扩展研究支持智慧城市统一管理的智慧小区原型系统。

具体内容包括：①研究支持泛在物联网设备和异构数据，支持强逻辑访问控制，支持多维度授权管理，具有隐私保护能力的基于标识的安全物联网互联互通架构；②结合安全态势智能管控、应用安全管理、网络分层安全管理、设备分级安全管理等安全保障技术，研制智慧城市安全保障技术架构；③研制支持大规模物联网对象分级管理与安全解析，物联网设备发现、识别和监控以及身份认证、密钥管理服务均支持 10 亿规模的安全物联网原型平台；④研制支持智慧城市统一管理与支持隐私保护的智慧小区和智



慧家庭适用的安全控制中心、安全网关、智能防火墙等原型系统，并通过权威部门测评，得到试点应用。

该课题所研制网络安全体系架构及平台示范系统基于其余四个课题研发的部分共性关键技术和理论；同时也为其余四个课题提供架构指导及系统验证。

课题二：无安全代理的大规模设备智能发现、感知和监控

该课题主要针对**关键科学问题一**“资源受限的智能感知标识”映射在感知层中的具体研究内容，研究大规模设备监控技术，实现在无安全代理条件下设备自动发现、识别及状态、行为智能感知。

具体研究内容包括：①研究无打扰、跨网跨域、主被动结合的物联网设备搜索技术，实现无安全代理条件下设备自动发现；②多维属性融合的设备识别模型，设备及行为特征自动提取和快速识别技术；③设备安全状态探测与行为智能推断方法，及数据安全感知机制；④研制安全监管子平台，支持 10 亿规模设备发现、识别和监控。

该课题为基于异构标识的安全互联网互联互通机制（课题三）提供可标识的设备，同时为构建系统平台与应用示范（课题一）提供相应技术支持。

课题三：基于异构标识的安全物联网互联互通机制与协议

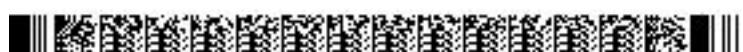
该课题主要针对**关键科学问题一**“资源受限的智能感知标识”与**关键科学问题二**“大规模泛在网络的安全异质互联”，研究多物联网管理域之间的受控互联互通机制与安全协议，提出基于异构标识的安全物联网互联互通架构。

具体研究内容包括：①海量物联网对象的标识提取及生成技术，基于多元特征生成多类型可靠标识；②在大规模物联网环境下且资源受限条件下基于标识的轻量级跨域身份认证、多维分级授权和数据隐私保护技术；③基于大规模异构标识的高效安全分层管理与跨域安全解析。

该课题为大连接复杂异构条件下的物联网一体化安全机制（课题四）提供海量物理对象互联、数据互通的基础安全机制与协议，同时为物联网互联互通安全架构（课题一）提供技术支持。

课题四：大连接复杂异构条件下的物联网一体化安全机制

主要针对**关键科学问题二**“大规模泛在网络的安全异质互联”在共性基础安全技术层面中的具体研究内容，在大连接、异构数据、时延复杂条件下，研究与节点融合的“感传存算”一体化安全机制：



具体研究内容包括：①多因子情境识别感知和安全异构数据融合技术，实现异构数据可信感知；②轻量级认证和密钥管理方案，实现大连接条件下的节点安全接入和通信隐私保护；③轻量级加密技术，实现异构数据的安全存储、计算和隐私保护；④云端融合、传算结合技术，优化协同任务分配，达到节点资源约束下的安全和性能优化平衡。

该课题为动态跨域的大规模分布式信任服务机理（课题五）提供基于云端融合、传算结合的共性安全技术，为研制安全物联网原型平台、智慧城市统一管理的智慧小区原型系统（课题一）提供一体化安全机制支持。

课题五：动态跨域的大规模分布式信任服务机理

该课题主要针对关键科学问题三“复杂跨域环境下的信任机理”在共性基础安全技术层面中的具体研究内容，针对物联网跨域服务信任问题，研究基于分布式共识的大规模跨域信任服务机理及关键技术。

具体研究内容包括：①基于国产密码算法，研究采用软件定义的方式实现管理域之间强逻辑隔离的安全机制；②基于分布式共识的跨域身份信息与认证技术，保障物联网数据完整性和可信性；③复杂管理域环境下的安全策略协商机制，保障协议安全性；④基于身份和角色的授权策略映射，保障访问控制与数据交换，支持时间、环境以及安全上下文敏感的授权管理。

该课题为研制安全物联网原型平台、支持智慧城市统一管理的智慧小区原型系统（课题一）提供动态跨域分布式信任服务机理技术支持。

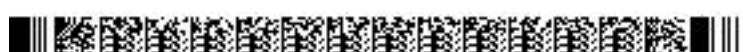
（二）项目各任务（课题）内容

1. 课题一：适应智慧城市与物联网安全目标的安全架构和应用示范

1.1 研究目标

建立一体化安全关键技术，构建适应智慧城市与物联网安全的模型和体系框架，研制安全物联网原型平台。研究目标包括

- 1) 从共性关键技术和安全需求出发，构建面向智慧城市与物联网安全为核心目标的安全架构。主要包括共性基础安全关键技术，同时提供数据服务层，计算存储层、网络层和感知层的关键技术。以此构建应用示范平台，支撑设备的智能发现与管理、



互联互通、跨域连接、存储管理、以及具有隐私保护功能的跨域信任数据服务。

- 2) 根据智慧城市的安全建设需求,研究智慧城市安全保障技术架构,从安全技术体系、管理体系、运维体系出发,设计一套完整的安全保障体系。
- 3) 在网络安全设施方面,提供防火墙,入侵防御,网站防篡改,安全审计,防病毒等服务。为物理与环境安全、系统安全、网络安全,数据和应用安全设计全方位的智慧城市安全保障体系。

1.2 研究内容

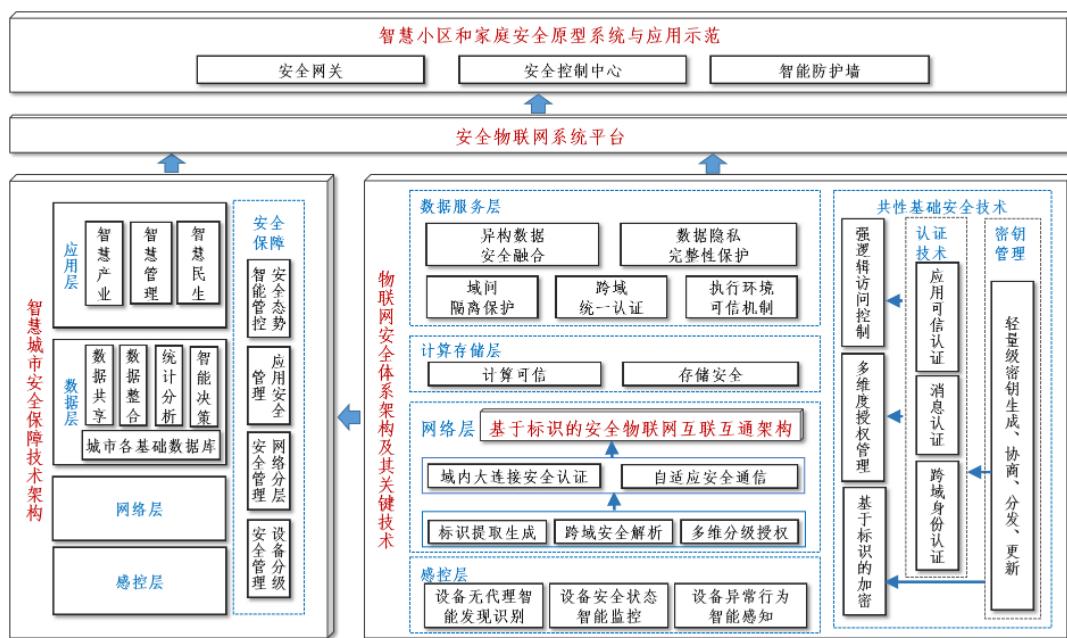
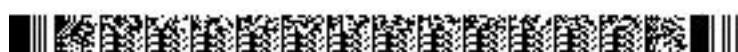


图 2.8 课题 1 研究内容

1.2.1 物联网安全体系结构及关键技术

- (1) **面向轻量级标识的强逻辑共性基础安全:** 研究轻量级密钥管理,包括密钥生成、协商、分发和更新机制。研究面向物联网设备的认证技术,包括跨域身份认证、消息认证和应用可信认证。最终实现基于标识的加密,多维授权管理和强逻辑访问控制。
- (2) **智能高维跨域的设备感控层:** 研究无代理的设备智能发现与识别,实现设备安全状态的智能监控和异常行为感知。特别是针对物联网设备的多维属性,建立多维跨域感知通道,对设备实现更智能,更细粒度和更高维度的管理与监控。
- (3) **面向异构大连接的网络层:** 研究标识提取生成技术,跨域安全解析技术,实现多维分级授权管理。面向网络大连接,研究域内安全认证,实现自适应安全通信,



构建基于标识的互联互通架构。

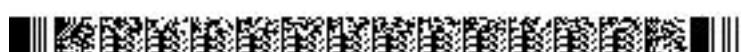
- (4) **安全可信的计算存储层：**计算存储层连接网络层与数据服务层，提供存储服务，为数据服务层提供计算支撑。研究面向数据服务的可信计算技术，以及网络层存储安全技术。
- (5) **跨域融合的数据服务层：**研究域间隔离保护机制，实现跨域统一认证。研究并建立执行环境可信机制，实现异构数据安全融合，确保数据隐私安全保护。

1.2.2 安全物联网原型平台

- (1) 原型平台构建：针对轻量级安全物联网平台需求，基于物联网安全目标模型和体系框架，设计一款依托于现有软硬件系统、安全关键技术的主要研究内容，进行验证评估的物联网原型平台。
- (2) 测试验证：针对感知层、网络层和应用层的软硬件需求，研究基于中移物联网平台或新研发物联网设备的物联网安全系统，解决大规模物联网对象的分级分层管理、安全解析、身份认证、密钥管理服务等测试验证需求。

- (3) 智能防火墙系统：基于安全大数据驱动的动态防御体系，研究针对全网威胁的智能防御，实现“用户态的协议栈以及一体化的安全引擎”，运用高性能的多模匹配算法，保证低延迟，高吞吐的报文转发；研究采用沙箱技术解决未知的文件型威胁，智能防火墙通过沙箱打造的虚拟环境，有效地阻断未知的文件型威胁。

1.2.3 智慧城市安全保障技术架构研究内容



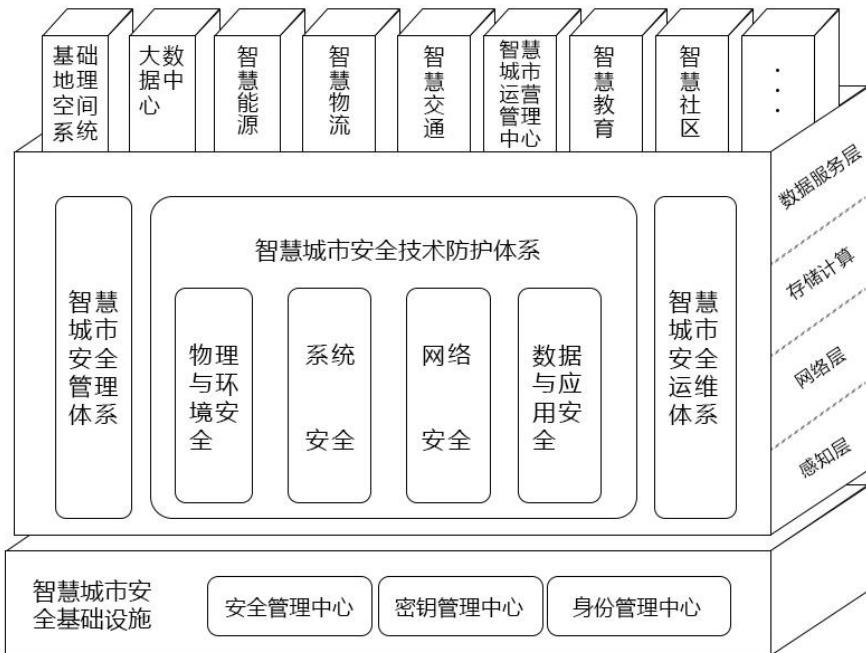


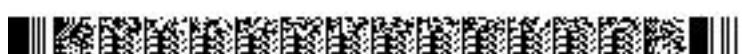
图 2.9 智慧城市体系架构与应用示范研究内容

(1) 构建智慧城市的分域控制体系：在总体安全保障技术架构上将按照等保分域保护思路进行，结合智慧城市环境的布局，从结构上划分为不同的安全区域，并通过统一的基础支撑平台来实现对智慧城市基础安全设施的集中管理，构建分域的控制体系。

(2) 构建纵深防御体系：针对智慧城市的安全防御，研究统一身份管理、访问控制、入侵检测、等多种技术和措施，并结合虚拟机防护等新的技术手段，实现业务应用的可用性、完整性和保密性，在此基础上实现综合安全管理。

(3) 分域安全强度保证：对于智慧城市环境和区域边界，采用分级管理方法，在通信网络上采取强度一致的安全措施，并采取统一的防护策略，使各安全措施在作用和功能上相互补充，形成动态的防护体系。实现各个级别信息系统的基本统一保护（如防病毒系统、审计系统），然后针对重点区域，采取高强度的保护措施。

(4) 分阶段建设智慧城市安全保障技术架构：总体上遵循当地《智慧城市规划》，拟分三个阶段实现示范应用：第一阶段实现基础的防护和 IaaS (Infrastructure-As-A-Service 基础实施即服务) 层安全，示范重点以传统安全为主，重点解决边界安全和网络安全，同时兼顾主机虚拟化安全和安全资源池的引入。第二阶段在实现数据充分共享后，重点考虑数据安全和多业务系统、多用户之间的安全隔离。第三阶段在统一管理后，实现安全管理运维标准和管理体系的建立。



1.3 拟解决的重大科学问题或关键技术问题

1.3.1 安全体系结构与平台

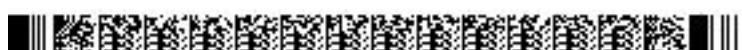
本课题围绕项目指南中提出的物联网安全管理体系结构、关键机制和关键应用的挑战，解决如下问题：

- (1) **面向物联网安全的共性关键技术。** 克服传统共性关键技术缺乏轻量级密钥管理功能，建立高效低开销的密钥生成、协商、分发和更新机制。在此基础上，提出面向物联网设备的认证技术，包括跨域身份认证、消息认证和应用可信认证。最终实现基于标识的加密，多维授权管理和强逻辑访问控制，并实现共性关键技术的支撑，为项目提供技术和服务保障。
- (2) **突破感知层智能、及细粒度、高维精准管控技术。** 首先克服传统管理缺乏智能发现与识别和精准管控能力的问题，在此基础上，实现设备安全状态的智能监控和异常行为的感知。特别是针对物联网设备的多维属性，提出并建立多维跨域感知通道，为实现更加智能，更细粒度和更高维度的管理与监控提供技术支撑。
- (3) **突破面向跨域大连接和网络标识的互联互通架构。** 克服传统网络层技术缺乏高效的标识提取生成技术，以及跨域安全解析技术，进而提出多维分级授权管理。在此基础上，提出域内大连接安全认证机制，研制自适应安全通信框架，进而构建基于标识的安全互联互通架构。
- (4) **突破可信并具有隐私保护的数据应用服务。** 克服传统数据服务缺乏高效准确的域间隔离保护机制，提出面向物联网设备的跨域统一认证，研究并建立执行环境可信机制，实现异构数据安全融合，确保数据隐私安全性保护。

1.3.2 智慧城市体系架构

(1) 突破基础设施安全统筹防护问题。 面向网络、系统和主机的安全防护需求，设计安全域和网络访问控制平台、统一监控与审计平台，和防病毒、补丁与终端管理平台等基础设施防护机制；解决网络、系统和部分应用软件的监控和审计问题，为云计算中心和各管理域提供监控和审计技术手段。

(2) 突破应用和数据安全体系统筹防护问题。 面向应用和数据存在的安全隐患，设计应用安全平台。突破总体层面统一设计、建设和管理的支撑平台和统一认证与授权管理平台关键技术。设计数据备份与冗灾体系，研究数据层面解决重要系统的数据备份和冗灾存在的问题，突破重要数据的完整性和可用性评估技术。



(3) 突破统一安全管理平台设计技术。研究覆盖智慧城市体系架构各个层面，设计统一安全管理功能体系。突破承载整体安全工作的软件和工作流支撑技术，从策略体系、组织体系、技术体系和运行体系等方面进行技术整合，形成承载整个智慧城市物联网安全体系的支撑平台。

1.4 考核指标及评测手段/方法

具体考核指标和评测方法详细见表 1 中的成果 1：“适应智慧城市与物联网安全目标的安全架构和应用示范”。

1.5 参加单位任务分工

课题由中国科学技术大学牵头，任务分工如下：

- (1) 子任务 1：物联网安全体系结构及关键技术。承担单位：中国科学技术大学、国家信息中心。
- (2) 子任务 2：安全物联网原型平台。承担单位：中移物联网公司。
- (3) 子任务 3：智慧城市安全保障技术架构及应用示范。承担单位：北京泰豪智能工程有限公司、北京奇安信科技有限公司。

2. 课题二：无安全代理的大规模设备智能发现、感知和监控

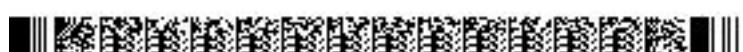
2.1 研究目标

针对智慧城市中大规模、异构物联网设备，提出一系列设备智能发现、感知和监控技术，实现在无安全代理条件下的设备自动发现、识别、行为智能感知。具体研究目标包括：

- 1) 研究无打扰、高效率、跨网跨域、主被动结合的大规模设备发现技术；
- 2) 研究多维属性融合的设备识别模型及方法；
- 3) 研究设备安全状态探测与行为智能推断方法，及数据安全感知机制；
- 4) 研制物联网安全监管子平台，支持支持 10 亿规模设备发现、识别和监控。

2.2 主要研究内容

主要研究内容如图 2.10 所示。



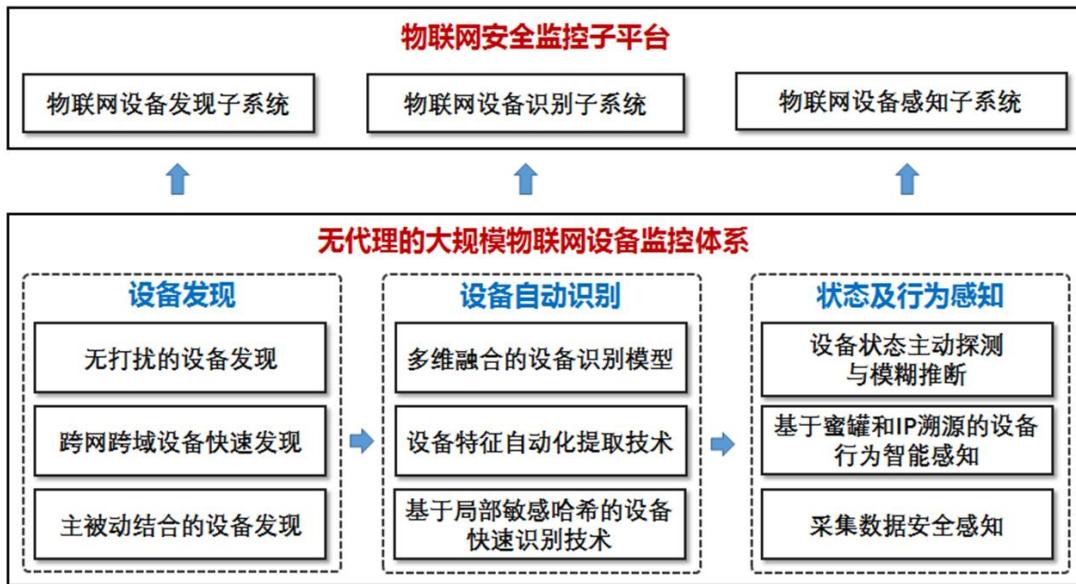


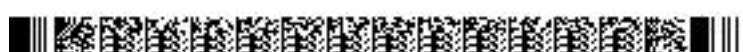
图 2.10 课题 2 主要研究内容

2.2.1 无打扰、跨网跨域、主被动结合的设备发现

- (1) **无打扰的设备发现技术:** 针对物联网设备的全分类目标, 研究基于决策树的多指纹模型的策略优化调度方法, 实现最佳的指纹模型使用次序, 以最小化设备精细化识别中的扫描遍历次数; 基于前述研究的探测报文变异能力和多指纹模型探测方案, 结合分布式扫描方法, 研究基于博弈理论的动态抗阻断扫描方法, 以提高发现防御体系内部物联网设备的能力。
- (2) **跨网跨域的设备快速发现技术:** 结合水平搜索、垂直搜索、任务分配和主机调度等机制, 研究低干扰、高效的全球设备层次式探测策略, 以及信息熵最大化的设备快速搜索方法; 结合内网穿透技术, 研究跨网跨域的设备快速搜索技术。
- (3) **主被动结合的物联网设备发现技术:** 针对物联网的私有协议, 研究物联网协议的深度解析和逆向技术; 基于物联网协议解析, 研究自动化的物联网设备流量还原技术; 基于流量分析, 研究物联网设备被动发现技术; 综合流量分析和设备主动探测, 研究主被动结合的物联网设备发现技术。

2.2.2 多维属性融合的设备识别模型及方法

- (1) **多维融合的设备识别模型:** 结合物联网设备的多维属性, 提出多维融合的设备识别指纹模型。研究基于深度学习的物联网设备精细指纹模型生成技术, 借助深度学习的隐特征、尤其是隐关联特征的抽取能力, 深度挖掘探测报文序列的显式特征和隐含特征, 拓展指纹特征空间, 提高不同种类物联网设备的区分度。



(2) 设备特征自动化提取技术：探讨物联网设备精细化识别流程、扫描地址空间压缩机制、精细化指纹自动提取、多指纹模型扫描的调度优化策略和抗阻断等技术，形成完整、可扩展的新技术体系与架构，并在此基础上形成各技术环节的评价指标体系，以指导后续研究工作的开展；基于自然语言处理和机器学习方法，研究海量设备的指纹自动化提取和识别技术。

(3) 设备快速识别技术：基于 Bloom-Filter（布隆过滤器）、Locality-Sensitive-Hashing(LSH, 局部敏感哈希)等技术，研究物联网设备特征与指纹库的快速匹配技术；研究层次式的物联网设备快速识别技术；采用半连接的无状态链接、地址散列等技术，研究分布式并行的物联网设备快速识别技术，实现大规模设备的快速识别。

2.2.3 设备安全状态探测与行为智能推断方法

(1) 设备状态主动探测与模糊推断：研究基于动态仿真的固件脆弱性分析技术；基于物联网设备远程可访问文件的安全性分析，研究能够发现多种脆弱性的主动探测方法；基于设备关联关系或漏洞信息匹配，研究信息不对称条件下的设备脆弱性模糊推断方法；研究安全可靠的物联网数据采集感知机制。

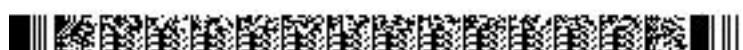
(2) 基于蜜罐和 IP 溯源的设备行为智能感知：基于恶意代码的传播特性，并结合 Honeypot(蜜罐)和 IP 溯源技术，研究网络空间中恶意物联网设备（即被利用物联网设备）的主动检测方法；基于同源行为特征分析，研究由恶意设备组成的僵尸网络的鉴别机制。

(3) 安全可靠的物联网数据采集感知：基于物联网设备上传数据报文中附带的其他信息，例如 WIFI 报文中的 CSI (Channel-State-Information 信道状态信息)，采用边信道分析方法，来区分正常设备上传数据与伪造者注入的数据，进而实现安全可靠的物联网数据感知和采集。

2.2.4 物联网安全监管子平台

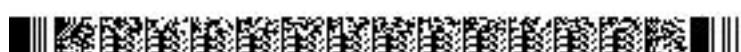
基于无打扰、跨网跨域、主被动结合的设备发现技术，研发物联网发现子系统、物联网识别子系统，以及物联网安全状态感知子系统，并将上述子系统集成为物联网安全监控子平台；在智慧消防等物联网应用场景，对提出的关键技术进行验证。

2.3 拟解决的重大科学问题或关键技术问题



本课题围绕项目指南中“研究大规模设备监控技术，实现在无安全代理条件下设备自动发现、识别及状态、行为智能感知”面临的挑战研究无安全代理的大规模设备智能发现、感知和监控技术，拟解决的重大科学问题或关键技术如下：

- (1) **异构、繁杂多样物联网设备的快速发现技术：**精确认别网络空间设备是物联网设备发现与识别的基本要求。物联网设备识别的核心技术之一是设备指纹的高效、低干扰提取。物联网设备类型繁多，每一类型的设备又包含上万的厂商和型号，造成设备之间的差异越来越小，设备特征交叉重叠，这使得构造不同指纹来区分海量设备越来越困难。现有的方法仅支持少量设备的识别，指纹模型单一，多采用人工方式，无法满足物联网环境下海量设备精准识别的需求，如何综合考虑设备的多维属性，自动化的提取设备指纹实现海量异构物联网设备的精确认别，是一个极具挑战的问题。同时，现有的设备搜索技术仅能快速检测主机存活性，未考虑复杂多样的应用场景，导致设备搜索的发现率低和发现的设备信息量不足。如何优化探测序列使用少量的探测包，保证在低打扰、高隐蔽前提下做到精准快速探测，并获取尽可能多的设备信息，是物联网设备搜索进一步需要解决的问题。因此，快速、精准的物联网设备发现与识别是需要解决的关键技术。
- (2) **信息有限条件下设备安全状态的模糊推断技术：**利用物联网设备进行网络攻击的事件频发，需要及时发现在线设备的脆弱性，及时检查在线设备是否被攻击被利用。检测设备是否被植入恶意代码，需要研究人员在获取设备控制权的条件下，对设备进程或流量进行深入分析，从而发现恶意行为或代码。因此，检测设备是否被恶意控制需要大量的检测信息。然而现有大规模在线设备的安全检测方法多通过轻量级的主动探测方式，难以获取设备的控制权，仅能获得设备部分协议的响应报文。在此如此有限的信息下检测恶意设备是非常困难的。并且，感染物联网设备的恶意代码通常会采取主动规避策略来隐匿其异常行为，进一步增加了在线恶意设备检测的难度。现有对恶意设备的主动检测，需要对已知恶意代码的行为特征进行建模，对感染未知恶意代码设备无能为力。因此，如何结合设备的特征和异常行为，实现对恶意设备的行为建模，以及如何在获取信息有限条件下，实现恶意设备在线检测是物联网安全需要研究的关键技术。



2.4 考核指标及评测手段/方法:

具体考核指标和评测方法详细见表 1 中的成果 2:“无安全代理的大规模设备深度感知和智能监控”。

2.5 参加单位任务分工

课题由中国科学院信息工程研究所牵头,任务分工如下:

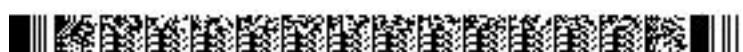
- 子任务 1: 无打扰、跨网跨域、主被动结合的设备发现。承担单位: 中国科学院信息工程研究所。
- 子任务 2: 多维属性融合的设备识别模型及方法。承担单位: 北京交通大学。
- 子任务 3: 设备安全状态探测与行为智能推断方法。承担单位: 太原理工大学,中国科学技术大学。
- 子任务 4: 物联网安全监管子平台: 承担单位: 北京富邦智慧物联科技有限公司,中国科学院信息工程研究所。

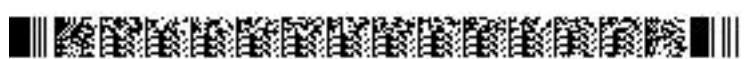
3. 课题三：基于异构标识的安全物联网互联互通机制与协议

3.1 研究目标

本课题主要基于异构标识实现安全互联互通机制与协议。研究目标包括

- 1) 基于设备网络地址、RFID 标签、环境传感器、摄像头和物理信道信息等多元特征, 提出可靠标识生成方法。
- 2) 支持海量物联网对象的异构标识管理架构, 设计异构标识解析系统跨域互联互通的融合方案, 形成异构标识管理与解析的安全机制。
- 3) 针对大规模泛在物联网中通讯协议异构、跨域安全数据路由协议缺失等问题, 基于海量物联网对象标识动态生成技术, 构建异构通讯协议安全融合机制、设计多层跨网域安全数据路由协议。
- 4) 面向异构标识实现基于国产密码算法的轻量级域内身份认证, 基于区块链技术的跨网域身份认证以及多元化数据隐私保护方法。
- 5) 面向大规模物联网跨域访问和授权管理问题, 提出基于异构标识的跨域多维分级授权和访问控制模型, 支持基于身份和角色的授权策略映射。





3.2 主要研究内容

主要研究内容如图 2.11 所示。

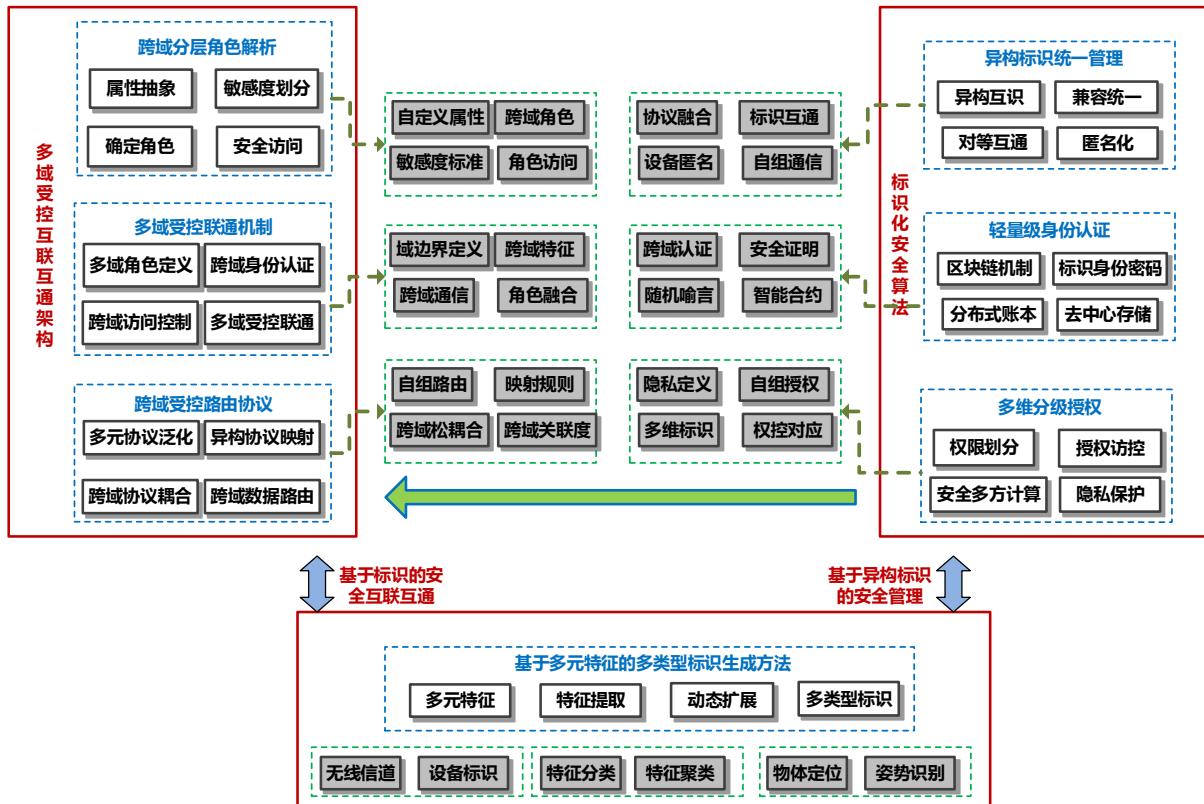


图 2.11 课题 3 主要研究内容

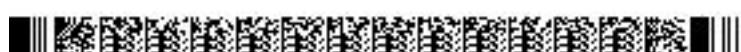
3.2.1 基于多元特征的多类型可靠标识生成方法

(1) 研究基于物联网设备的多元标识生成和验证方法, 包括: 1) 异构物联网设备的多元特征提取和识别的理论和方法; 2) 基于相位信息的设备定位技术和姿态识别技术; 3) 结合设备位置信息标识和身份标识提出快速验证和授权机制; 4) 基于多元特征的统一标识生成方法。

(2) 研究基于无线信道特征的标识生成方法和轻量级密钥交换方法, 包括: 1) 提出稳定无线信道特征标识提取方法; 2) 根据不同信道特征, 设计轻量级标识验证方法; 3) 基于信道特征标识生成方式, 提出快速、轻量级密钥交换方法。

3.2.2 基于标识的异构通信协议互联机制和数据安全路由协议

(1) **异构通讯协议安全融合互联机制:** 包括 1) 多元协议泛化: 将多元异构的通讯协议中通讯要素剥离、抽象化、模块化, 从语法、语义、时序等方面建立一套完整、



自治的泛化通讯协议，用于汇聚节点和网关节点等，保证节点在使用不同通讯协议时能找到数据交互的互联网实体对象，从而保证节点间的逻辑联系。2) 异构协议映射：建立泛化通讯协议，研究诸如 RFID、红外、ZigBee、Bluetooth、GPRS、3G、4G、Wi-Fi、NB-IoT、LoRa 等异构通讯协议与泛化协议之间的映射关系，从语法、语义、时序等层面保证信息交互的对等性、交互性与实时性。

(2) 多层跨域受控安全数据路由协议：包括 1) 域内协议耦合：针对同一管理域中可能存在的多个异构子网，研究域内不同数据路由协议在子网间的耦合，以保证同管理域节点数据流通。2) 跨域数据路由：在管理域间建立统一的多层次跨域受控安全数据路由协议，以降低路由开销、提高路由效率、增加网络容量。具体如图 2.12 所示。

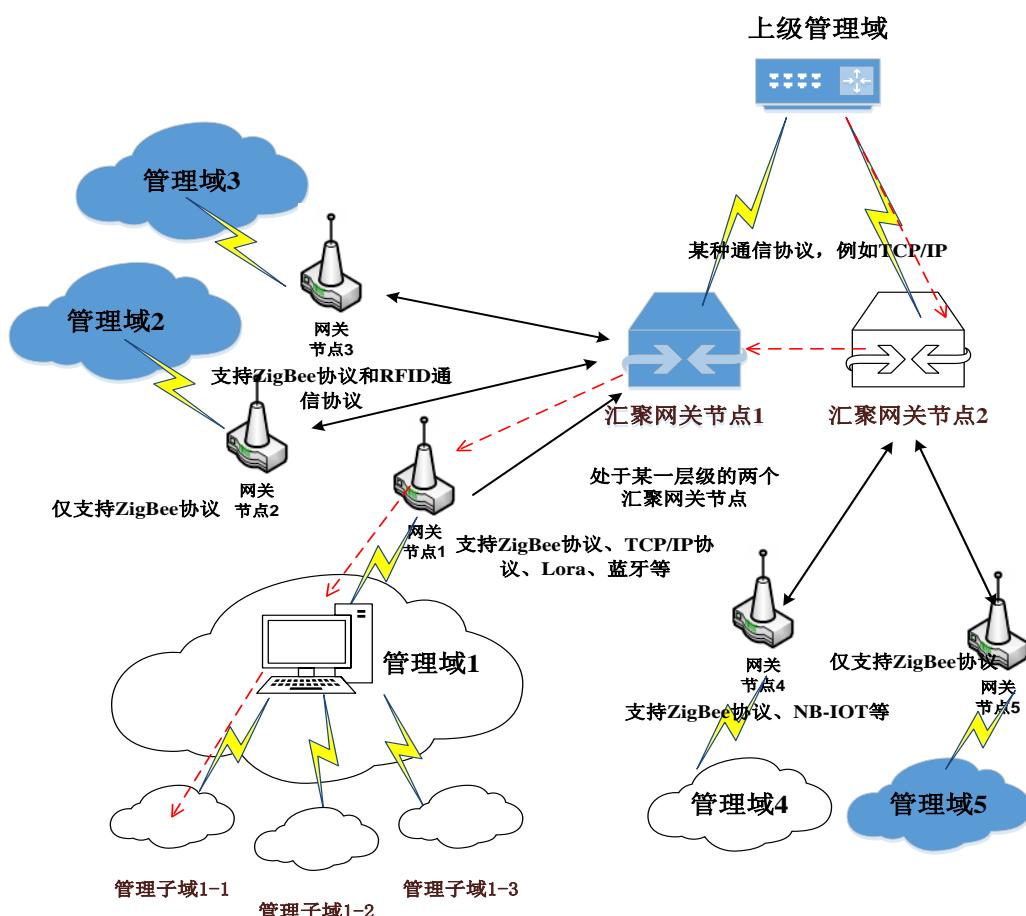
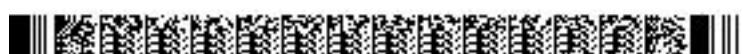


图 2.12 管理域协作关系

3.2.3 基于标识的轻量级域内及跨域身份认证和数据隐私保护机制

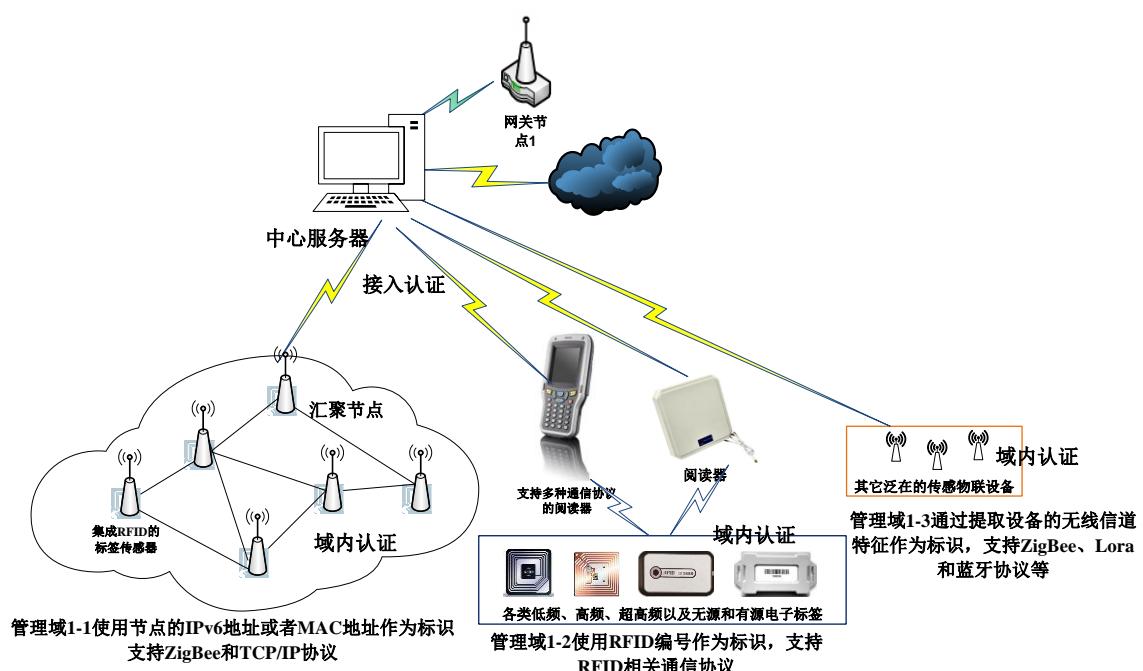
(1) 基于标识的域内轻量级身份认证：针对物联网标识认证协议缺乏严格的安全性证明问题，基于计算复杂性理论，在随机预言模型下，提出满足非对称密码算法系统要求的可证明安全的标识认证模型。根据物联网设备标识的唯一性，研究基于国产 SM9



标识密码算法的轻量级身份认证协议，结合 CHAP (Challenge-Handshake-Authentication-Protocol 询问握手认证协议) 实现强身份的标识认证。

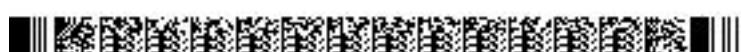
(2) 基于区块链的跨域身份认证：集中式 PKI (Public-Key-Infrastructure 公钥基础设施) 认证方式难支持跨域认证，研究基于区块链的点对点身份认证机制。研究消除工作量证明的基于 PBFT (Practical-Byzantine-Fault-Tolerance 实用拜占庭容错算法) 共识机制的私有区块链和联盟区块链技术，并结合智能合约技术，实现物联网跨域设备的轻量级分层分级认证。

(3) 针对标识在物联网应用中存在的隐私威胁，研究基于 PIN 认证标识的支持口令保护的终止命令方法和支持睡眠命令的改进方法，以解除设备和标识之间关联性。研究基于有限随机重写标识序列号及可替换标识组的标识变换方法。研究基于安全多方计算的隐匿标识获取方法。具体如图 2.13 所示。



3.2.4 安全互通的异构标识跨域对等解析与分层管理

(1) 支持异构标识的对等解析互通架构：研究基于区块链、DHT 的异构标识对等解析互通机制，研究标识映射关系的防篡改方法。实现基于“DHT+树”结构的高效分层



管理。解决物联网中多个异构的标识体系在多根互通、对等解析的情况下，标识映射记录在同步时的不一致性、安全和隐私保护等问题。

(2) 标识解析的安全机制：研究标识解析的权限保护、查询的权限设置、标识解析应答和映射关系的不可篡改和防止映射关系被劫持等安全机制。研究标识解析的隐私保护技术，从标识解析查询者、解析响应记录等多个角度研究基于身份、属性、K 匿名等技术的分级权限管理，有效保护解析过程中的信息。

3.2.5 基于标识的跨域多维分级授权和访问控制机制

(1) 研究大规模物联网跨域多维授权及访问控制模型，建立感知节点标识、管理域标识、访问者标识及角色、感知节点及访问者的多维属性与访问者权限的动态映射关系，明确感知节点、管理域、密钥管理中心、访问者等实体功能及交互；针对跨域多维授权的细粒度划分问题，研究基于属性的加解密算法和基于标识的加解密算法的协同实现方法，实现标识、角色、属性在加解密过程中的自动映射与融合应用。

(2) 研究大规模物联网层簇式树形授权管理结构、用户注册流程、用户分级原则、管理域分级原则、访问授权原则，明确物联网跨域访问时多维属性授权与分级访问控制的协调原则及对应关系。

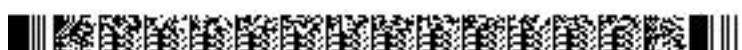
(3) 研究多维分级授权及访问控制模型的安全性证明问题，构造形式化敌手模型，利用概率论和计算复杂性理论，把对多维授权和分级访问控制模型的攻击规约到已知困难问题或安全假设来证明模型安全性。针对物联网多维分级授权和访问控制模型的实验验证问题，研究如何采用 SM9 国家标准密码算法实现基于标识的授权及访问控制，采用双线性对映射构造多维属性加解密算法及分级访问控制机制。

3.3 拟解决重大科学问题或关键技术问题

本课题拟解决的重大科学问题及关键技术如下：

(1) 基于异构标识的物联网互联互通架构及跨域通信和解析：在资源受限的物联网对象中，基于多元特征提取技术，解决轻量级可靠标识的生成问题。基于多元协议泛化技术，解决大规模泛在网络中异构通讯协议安全融合及多层跨域数据路由问题。最终实现海量物联网对象的标识化管理及异构标识跨域解析互联互通架构的融合机制。

(2) 基于异构标识的安全认证、跨域多维授权和隐私保护：针对物联网对象资源受限、易受攻击的特性，面向上层网关控制节点快速相互认证、分层分级管理需求，采用分布



式快速响应的轻量级安全机制，解决域间及跨域身份认证问题；针对隐私泄露及窃取等安全威胁，实现跨域的数据隐私保护。采用身份、角色、属性深度融合的细粒度自适应访问控制机制，解决大规模物联网跨域多维分级授权的模型构建与安全性证明问题。

3.3 考核指标及评测手段/方法

具体考核指标和评测方法详细见表 1 中的成果 3：“基于异构标识的安全物联网互联互通机制与协议”。

3.4 参加单位任务分工

本课题由南京邮电大学牵头，任务分工如下：

- 子任务 1：基于多元特征的多类型可靠标识生成方法。承担单位：清华大学。
- 子任务 2：基于标识的异构通信协议互联机制和安全数据路由协议。承担单位：合肥工业大学。
- 子任务 3：基于标识的轻量级域内及跨域身份认证和数据隐私保护机制。承担单位：南京邮电大学。
- 子任务 4：异构标识的高效安全分层管理和跨域安全解析。承担单位：中国科学院计算机网络信息中心。
- 子任务 5：基于标识的跨域多维分级授权和访问控制机制。承担单位：北京科技大学。

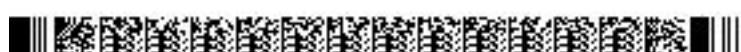
4. 课题四：大连接复杂异构条件下的物联网一体化安全机制

4.1 研究目标

针对当前物联网普遍存在的大连接、异构数据、时延复杂等场景，研究与节点融合的“感存算”一体化安全机制，具体包括：

- 1) 研究面向异构数据的可信感知、安全存算机制；
- 2) 研究面向大连接、时延复杂条件的安全传输机制；
- 3) 研究面向物联网节点的安全和性能优化机制。

综合以上研究成果，本课题旨在将大规模节点的安全接入和通信隐私保护、异构数据的可信感知和安全存算以及基于云端融合和传算结合的性能优化技术整合为一个



有机整体，构建一体化的安全机制，保障物联网及其节点的安全防护，并为相关原型系统的研发提供技术支撑。

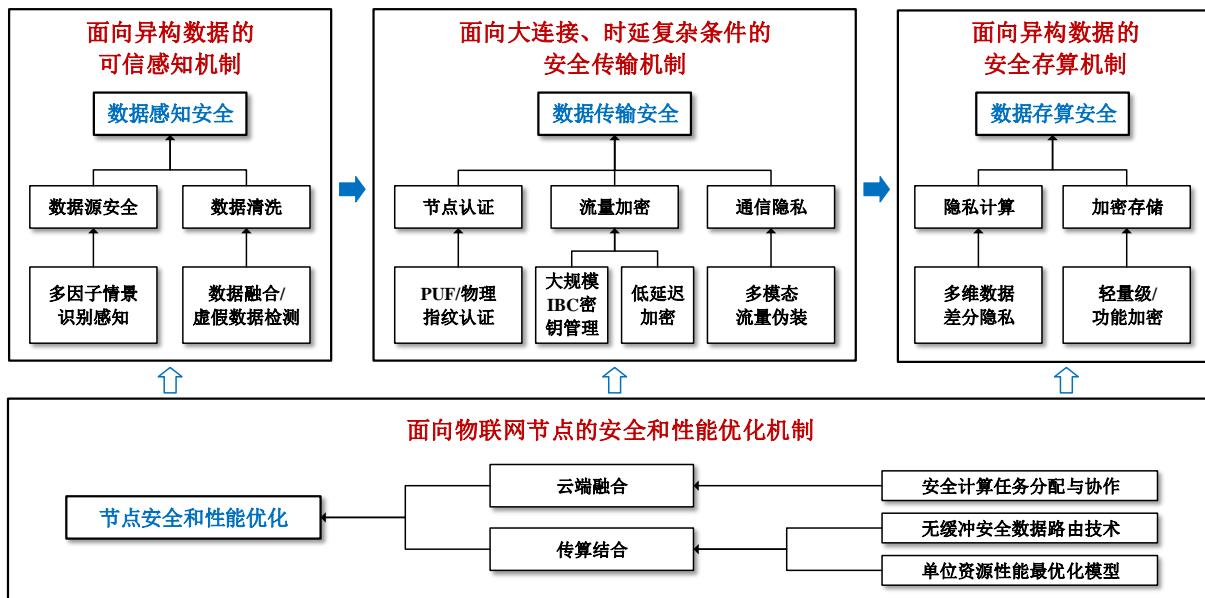


图 2.14 课题 4 的主要研究内容

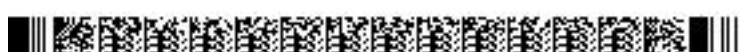
4.2 主要研究内容

课题四主要研究内容如图 2.14 所示：

4.2.1. 面向异构数据的可信感知机制

首先利用多因子情境感知技术实现对感知数据源可靠性的持续检测，其次在虚假注入数据识别的基础上实现对感知数据本身真实性的验证。

- 多因子情境识别感知技术：**为保障物联网感知数据源的可靠性，研究适用于物联网的多因子情境识别技术。针对节点的目标感知环境，通过综合利用 WIFI、蓝牙、Zigbee 等无线信号信道状态在时域、频域上的互相关矩阵，挖掘感知环境的有效特征，实现对环境的可信识别。针对物联网应用中日益普及的智能终端、可穿戴设备等便携装置，研究以人作为感知数据源的持续认证技术。通过利用设备中的加速度、陀螺仪、磁场等传感器，隐式地识别人的行特征，从而实现对感知数据源的可信识别。
- 安全异构数据融合技术：**物联网感知节点分布广泛、种类众多，且通常在无安全监测的情况下工作，存在安全隐患。为保障感知节点所采集数据的真实性和有效性，利用分布式多传感器可信物联网节点，对多元异构数据进行融合、聚类，并对不同节点、不同传感器数据交叉状态进行检测，识别注入的虚假异常。



数据，实现对感知数据的有效清洗，保证数据融合的安全性。

4.2.2. 面向异构数据的安全存算机制

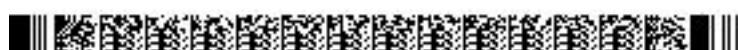
围绕物联网节点感知数据的汇聚、存储和计算三个阶段，研究相应的数据安全与隐私保护技术。

- **数据汇聚机制：**针对用户感知数据汇聚时存在隐私泄露风险的问题，研究基于差分隐私的感知数据处理机制，提出敏感度计算方法，进而研究隐私感知的混合异构数据存取技术，在满足用户隐私需求的前提下，降低差分隐私噪声，保证汇聚数据的准确度。
- **数据存储机制：**针对感知数据存储存在的隐私泄露风险，研究基于轻量级加密的数据存储机制，实现感知数据的安全存储。面向海量感知数据的分布式存储，设计基于统一角色集定义的访问权限协作机制，确保分布式数据访问控制安全。
- **数据计算机制：**针对加密数据的统计分析需求，研究基于功能加密的密文计算技术，以及基于该加密算法生成的密文数据的索引、访问和搜索技术，实现感知数据的安全计算。

4.2.3. 面向大连接、时延复杂条件下的安全传输机制

针对大连接、时延复杂条件下的安全传输，本课题主要围绕节点的接入认证、数据的加密传输以及通信隐私保护三个方面进行研究。此外，针对大连接条件下密钥管理难的问题，设计基于标识的大规模密钥管理机制，实现密钥的有效管理。

- **轻量级认证技术：**针对大连接条件下异构节点的安全接入问题，利用节点硬件物理特征的不可克隆性，研究基于 PUF、物理指纹的轻量级认证技术，通过提取或引入物理构造的随机差异性特征生成唯一标识，实现节点的安全接入。相较于传统的基于证书的认证机制，该认证技术更为轻量级，可兼容计算资源、功耗受限的节点，同时也提高实时响应速度。
- **低延迟数据传输技术：**针对现有的标准加密算法无法满足物联网中低延迟数据传输需求的问题，研究基于低延迟加密算法的自适应数据传输技术，根据节点本身的硬件资源，对密码置换盒位数、加密轮数等要素进行评估，在保证一定的安全性的前提下简化算法，从而减少计算耗时，以满足物联网中低延迟的数据传输需求。在此基础上，研究多路径数据传输机制，进一步提高数据吞吐量，降低传输延迟。



- **多模态流量伪装技术：**针对感知数据量、感知频率等侧信道信息带来的隐私泄露风险，在链路流量变换、流量正规化等方法的基础上，研究自适应的多模态流量伪装技术，通过对具体应用隐私保护需求的分析，自适应地对流量中包间隔到达时间、包大小、持续时间、传输包总数、连接的开始和结束时间、负载流量速率等特征进行调制，实现对流量模式的最优伪装，有效抵御侧信道攻击。
- **大规模密钥管理机制：**针对大连接条件下物联网节点数量众多导致密钥管理难的问题，以简化密钥管理和减少系统通信量为目标，提出基于节点标识的大规模 IBC（Identity-Based-Cryptography 基于身份的密码体系）密钥管理机制。

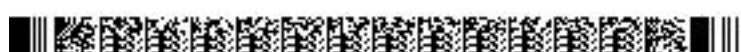
4.2.4. 面向物联网节点的安全和性能优化机制

在面向物联网节点的安全和性能优化方面，从物联网节点和云服务器全局考虑，设计面向大连接、时延复杂的云端融合机制；针对节点本地网络资源、功耗受限难以负荷安全计算任务的传输开销问题，研究面向节点资源受限的传算结合机制。

- **面向大连接、时延复杂的云端融合机制：**在物联网大连接、时延复杂条件下，重点针对不同时延需求的安全计算任务，从云服务器和端节点全局考虑，设计基于任务协作的云端融合机制。通过综合考虑云服务器和端节点的任务处理能力、云-端传输时延以及安全等级需求，优化合理分配安全计算任务，从而有效降低任务响应时间，实现安全和性能优化平衡。
- **面向节点资源受限的传算结合机制：**针对节点本地网络资源、功耗受限难以负荷安全计算任务的传输开销，研究端节点之间以及端节点与云服务器之间无缓冲的安全数据路由技术，并设计一套节点自主的动态传算结合机制，充分利用本地计算资源。通过评估并量化到达任务的资源需求，考虑资源和系统负载变化，构建在节点计算、存储、带宽、能耗等约束条件下的资源性能优化模型和平衡算法，并进一步研究动态自适应的安全计算任务分割策略，从而高效完成安全计算任务。

4.3. 拟解决的重大科学问题或关键技术问题：

- **物联网应用导向的用户隐私保护机制：**由于物联网节点的泛在性及所采集、传输数据的敏感性，数据隐私和通信隐私保护是本课题的基础问题。在数据隐私方面，经典差分隐私机制无法适用于物联网中的复杂应用场景和多维异构数据，因此如何针对不同的应用功能需求设计隐私保护机制，优化隐私和



功能权衡是本课题需要解决的一个关键技术问题。在通信隐私方面，为有效抵御侧信道攻击，需要进行流量模式的伪装。如何针对物联网应用时延复杂、数据异构和用户隐私保护需求各异的特点，自适应地进行最优流量伪装策略选择和参数配置，以实现服务质量与隐私保护的优化平衡也是本课题需要解决的一个关键技术问题。

- **面向物联网节点的安全和性能优化机制：**在物联网大连接、时延复杂条件下，如何从云服务器和端节点全局考虑设计基于任务协作的云端融合机制，如何针对节点本地网络资源、功耗受限问题设计动态传算结合机制，以高效利用资源、降低安全计算任务响应时间，实现安全和性能优化平衡是本课题需要解决的关键技术问题。

4.4 考核指标以及评测方法：

具体考核指标和评测方法详细见表 1 中的成果 4 “大连接复杂异构条件下的物联网一体化安全机制”。

4.5 参加单位任务分工

子任务 1：面向异构数据的可信感知机制 东南大学、北京大学

子任务 2：面向异构数据的安全存算机制 东南大学、西南大学

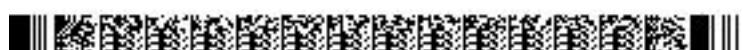
子任务 3：面向大连接、时延复杂条件下的安全传输机制 上海汉邦京泰数码技术有限公司、东南大学

子任务 4：面向物联网节点的安全和性能优化机制 西南大学、中国科学技术大学

5. 课题五：动态跨域的大规模分布式信任服务机理

5.1 研究目标

课题拟将物联网、区块链、密码学和软件定义网络等新技术与智慧小区、智慧家庭等智慧城市领域的诸多环境进行融合，在复杂跨域环境下的信任挑战下，主要研究从“隔离—协作—互信—管控”四个阶段入手，形成动态跨域的大规模分布式安全信任机制与管理系统，保障跨服务域环境通信的可靠性和数据的隐私性，提升智慧小区和智慧家庭的数字化、智能化、网络化和安全化水平。



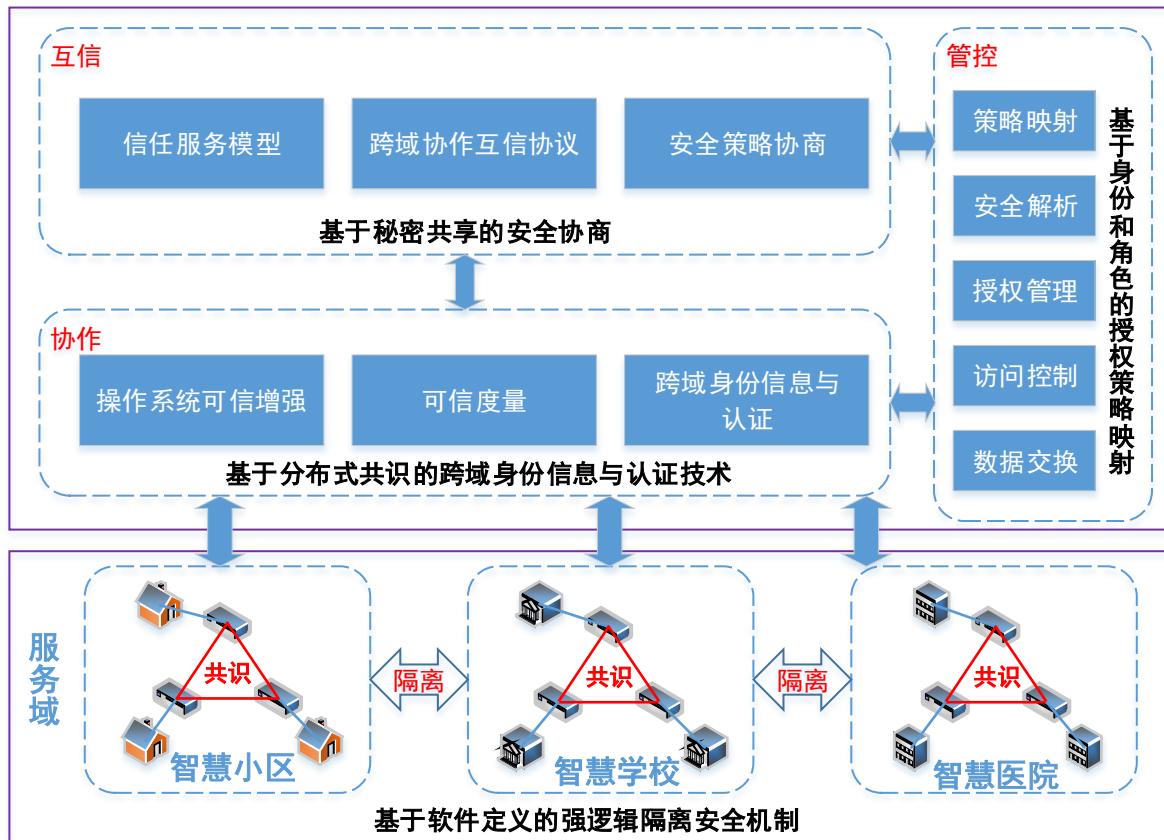


图 2.15 动态跨域的大规模分布式安全信任机理的总体设计图

5.2 研究内容

5.2.1 隔离阶段

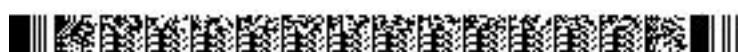
(1) 物联网节点之间的强逻辑隔离技术

研究基于软件定义的强逻辑隔离安全模型：面向两个或多个物联网节点之间数据的隐私性，将物联网节点作为最小的研究单位，研究基于软件定义的强逻辑隔离安全模型。分离物联网节点的控制平面与数据平面，采用软件定义方法，基于国家标准密码算法，面向物联网节点的控制平面设置和下发逻辑策略。物联网节点在通信时，数据流必须符合物联网节点控制平面的逻辑策略，实现对网络数据的隔离控制。

(2) 面向跨服务域的强逻辑隔离技术

研究面向物联网服务域的强逻辑隔离安全机制：在物联网服务域内部实现分布式共识的基础之上，将服务域作为最小的研究单位，针对跨服务域数据的隐私性问题，在基于软件定义的强逻辑隔离安全模型的基础之上，基于国家标准密码算法，研究面向物联网服务域的强逻辑隔离安全机制，保证跨物联网服务域初始状态数据的隐私性。

5.2.2 协作阶段



(1) 物联网操作系统可信增强技术

研究物联网操作系统的可信增强技术：面向两个或多个物联网节点之间数据的隐私性，将物联网节点作为最小的研究单位，针对物联网节点操作系统不可信的问题，研究物联网节点操作系统可信增强技术。针对物联网操作系统启动时可信性问题，研究面向物联网节点操作系统的可信启动机制，从物联网节点加电开始，通过一级度量一级、一级信任一级的方式，保障物联网节点操作系统整个启动过程的可信性。

(2) 跨物联网服务域的可信度量技术

研究跨物联网服务域的可信度量技术：针对每个物联网节点操作系统在运行过程中，从两个方面研究跨物联网服务域的可信度量技术。针对物联网节点的关键寄存器、关键内存区域等敏感数据的可信性问题，研究面向物联网节点操作系统的可信度量技术，通过制定和下发策略的方式，保障物联网节点运行时的可信性；面向服务域无可信第三方的场景，通过服务域内“互相监督”的方式，研究跨物联网服务域的可信度量技术，保障整个物联网服务域的可信运行。

(3) 跨服务域的身份信息与认证技术

研究基于分布式共识的双向多因素认证技术：在物联网服务域自身可信运行的基础之上，针对跨服务域连接身份信息不可信的问题，分别从身份信息和平台配置两个方面研究基于分布式共识的双向多因素认证技术。针对跨服务域连接发起时的身份可信性问题，研究双向的身份信息认证技术，保证跨服务域连接之前身份信息的可信性；针对跨服务域平台配置不可信的问题，保证跨服务域连接之前平台配置信息的可信性。

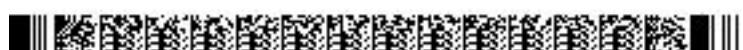
5.2.3 互信阶段

(1) 跨服务域的安全协商技术

研究基于秘密共享的安全协商：以保证服务域之间连接时的密钥管理和安全策略协商为目标，针对资源受限的物联网设备密钥分配响应速度，研究基于秘密共享的轻量级域内密钥管理机制；针对消除对可信第三方的依赖问题，研究基于身份的无可信第三方域间密钥管理方案，通过分布式秘密共享建立顶层服务域间的信任机制，通过基于身份的密钥算法实现无证书的跨域密钥协商；针对密钥协商的效率和通信双方的隐私保护矛盾，研究复杂服务域下的安全策略协商协议。

5.2.4 管控阶段

(1) 异构物联网的安全解析机制



研究面向跨域异构物联网的安全解析机制：在跨物联网服务域的场景下，针对物联网节点操作系统、应用软件的版本、制作标准等平台配置差异产生的语义兼容问题，研究面向异构物联网的安全解析机制，确保跨物联网服务域安全协议语义的一致性和同步性，保证跨服务域安全上下文的安全性。

(2) 跨服务域的授权策略映射技术

研究基于身份和角色的授权策略映射技术：在保障安全解析正确性的基础上，面向不同角色的服务域划分不同的权限和不同的安全等级，同时保障权限分配的实时性，研究基于身份和角色的授权策略映射技术，在确保授权管理正确性的基础上有效的提升了实时响应速度。

5.2.5 动态跨域的大规模分布式安全信任机制与管理系统

(1) 面向跨服务域的系统实现

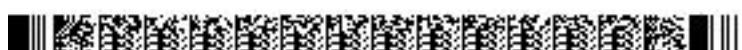
结合“隔离-协作-互信-管控”四个阶段的研究成果，构建动态跨域的大规模分布式安全信任机制与管理系统。拟采用智能网关作为管理系统的实现方式，主要包括四部分内容：采用分布式共识技术，保障物联网服务域内部数据的一致性；采用基于软件定义的强逻辑隔离技术，保障物联网服务域之间数据的隐私性；采用协作互信协议，保障物联网服务域之间通信的可信性；采用基于身份和角色的授权策略映射技术，保障物联网服务域之间通信的可控性。

5.3 拟解决的重大科学问题或关键技术问题

(1) **物联网服务域之间的信任服务机制：**传统智慧小区、智慧家庭之间的安全性保证是通过统一的管理机制实现完成。与传统的跨域安全信任机制不同的是，基于分布式的思维，面向复杂跨域的应用场景，从“隔离-协作-互信-管控”四个阶段入手，设计大规模跨域信任服务机理是本课题的一个关键技术问题。

(2) **物联网服务域之间初始状态的强逻辑隔离：**在物联网的服务域中，每个服务域初始状态容易造成重要数据的隐私泄露问题，是一个重要的技术问题，因此需要基于国家标准密码算法，结合软件定义的方法，设计物联网服务域之间初始状态的强逻辑隔离安全机制，保障在服务域之间的初始状态为彼此“强隔离”，是一个重要的技术挑战。

(3) **物联网服务域之间连接时的双因素认证：**在传统安全网关中，缺乏对安全网关系统运行时的安全性保障机制，因此如何增强安全网关操作系统的可信性是一个重要的技



术问题；另外，在安全网关长时间运行时，需要每时每刻都要保障系统的可信运行，如何设计安全网关操作系统的可信度量机制，是一个重要的技术问题；在安全网关可信运行的基础之上，在不同服务域互联时，还要证明用户身份的可信性，将用户身份可信和安全网关运行可信结合起来的双因素认证机制，是一个重要的技术问题。

(4) 资源受限环境下针对复杂服务域的轻量级的安全协商机制：在传统的PKI安全体制中，需要统一的可信第三方负责公私钥的管理机制。如何在无可信第三方情况下，研究建立基于身份的顶层服务域间信任关系，是实现跨越信任服务的核心技术问题；另外，在资源受限的情况下，建立基于秘密共享的高效域内密钥协商机制，是一个急需解决的技术问题；在复杂服务域下，如何兼顾性能与隐私保护的安全策略协商机制，也是一个重要的技术问题。

5.4 考核指标及评测手段/方法

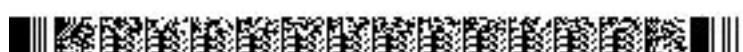
具体考核指标和评测方法详细见表1中的成果5：“基于分布式共识的大规模跨域信任服务机理及关键技术”。

5.5 参加单位任务分工

课题由清华大学牵头，任务分工如下：

- 子任务1：基于软件定义的强逻辑隔离安全机制。承担单位：清华大学、北京理工大学。
- 子任务2：基于分布式共识的跨域身份信息与认证技术。承担单位：上海交通大学。
- 子任务3：基于秘密共享的安全协商。承担单位：中国科学技术大学。
- 子任务4：基于身份和角色的授权策略映射。承担单位：清华大学。

子任务5：动态跨域的大规模分布式安全信任机制与管理系统。承担单位：清华大学、北京理工大学、中兴通讯。

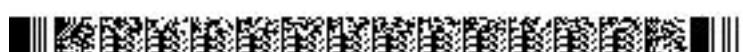


四、主要创新点

创新点 1：物联网安全系统结构的柔性可扩展理论与方法。面向大规模、异构、资源受限的物联网节点，提出无安全代理设备发现、识别与感知理论；提出数据驱动、云端结合的分级分层跨域安全体系架构；提出软件定义安全域边界、秘密共享的协作机理、分布式共识和功能加密的互信基础理论。实现高可靠、可扩展、资源适配的动态跨域安全机制。

创新点 2：轻量级智能安全机制。面向异构多源设备，设计跨层结构下指纹智能提取、计算、聚合、存储方法。提出基于特征相似度的设备脆弱性智能推断方法，设计低干扰、高效的层次式设备搜索方法，实现海量异构设备快速精准发现和无安全代理智能感知。提出轻量级密钥管理方法，实现身份认证和隐私保护安全机制。

创新点 3：物联网安全智慧城市一体化应用示范。面向国家新型智慧城市建设要求，将①基于标识的安全物联网互联互通架构，②绿色、智能、开放的物联网安全体系架构，③智慧城市安全保障总体技术架构及关键技术，应用在智慧城市统一管理的智慧小区或智慧家庭等行业并进行应用部署。相较于现有行业系统，能够有效实现连接设备超过 100 万台，接入家庭超过 20 万户，社区超过 1000 个，为基于物联网的智能化、柔性化、开放的城市管理提供应用示范。



五、预期经济社会效益

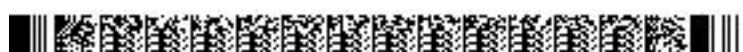
本项目面向物联网节点计算能力、体积、功耗等限制，大规模泛在异构连接和复杂跨域的智慧城市应用需求，研究“绿色、智能、开放”的物联网与智慧城市安全体系架构及其关键技术，构建安全物联网系统平台，实现智慧小区和智慧家庭原型系统和应用示范系统。项目的实施将带来显著的科学价值、社会、经济、生态效益。

1. 科学、技术、产业预期指标

项目的研究将形成物联网安全体系架构及关键技术，指导智慧城市安全保障技术构建和智慧小区智慧家庭原型和示范系统的建立，预计实现连接设备超过 100 万台，接入家庭超过 20 万户，社区超过 1000 个，实现基于物联网的智能化、柔性化、开放的城市管理的应用示范。

项目将突破物联网感知层关键技术，形成无安全代理条件下设备自动发现、识别及状态、行为智能感知技术，构建物联网安全监管子平台，支持 10 亿规模的物联网设备发现、识别和监控。解决基于多元特征的海量物联网对象标识提取及标识生成技术，建立大规模物联网环境中资源受限条件下基于标识的轻量级跨域身份认证、多维分级授权、数据隐私保护技术、分层管理与跨域安全解析技术，实现多物联网管理域之间的受控互联互通。在物联网大连接、异构数据、时延复杂条件下，突破多因子情境识别感知和安全异构数据融合技术，基于 PUF、物理指纹等技术的轻量级认证、融合差分隐私的同态轻量级加密技术。针对物联网跨域服务信任问题，基于软件定义实现管理域之间强逻辑隔离的安全机制，保障管理域之间的机密性，实现基于分布式共识的跨域身份信息与认证技术，保障管理域互联时的数据完整性和可信性；构建基于秘密共享的安全协商，实现复杂管理域环境的安全策略协商机制；面向大规模动态跨域的物联网环境，建立基于身份和角色的授权策略映射，保障跨管理域的访问控制与数据交换，支持时间、环境以及安全上下文敏感的授权管理，时间粒度不大于 1 分钟。

根据《2017 中国工业物联网白皮书》估计，仅 2016 年，物联网领域就形成了 1 万亿元人民币的产业规模，预计到 2020 年将达到 1.8 万亿规模。项目的实施将有效推动物联网安全架构、关键技术的发展与应用示范系统的研发、部署和推广，尤其将推动智慧城市安全保障、智慧小区、智能家居等领域应用的快速发展，占据物联网产业 25%以上的规模，预计 2020 年具备 4500 亿以上的产业规模。



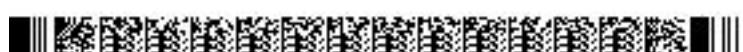
2. 科学价值、社会、经济、生态效益

项目的开展将形成拥有独立自主知识产权的核心技术体系，有效提升物联网安全核心技术水平，增强我国在物联网领域的核心竞争力；推动国内外物联网安全技术标准的制定，引领国际物联网安全技术的发展。

项目的研究将增强国家信息安全防护能力，促进网络信息安全人才培养。一方面，通过对项目研究提升我国物联网安全防护能力，建设和完善物联网应用系统，有效保障物联网各类资源的安全性；另一方面，项目将充分发挥高校牵头优势，通过产学研深度融合，培养物联网与智慧城市安全技术领域高端科研人员、技术技能人才与复合型人才，预期培养一批物联网领域高精尖人才和创新团队。

项目的研究将有效促进我国物联网产业化发展，助力“互联网+”以及“中国制造2025”国家战略的实施。将研究成果应用于智慧城市安全保障，智慧小区与智能家居管理，可以有效降低管理的人力、资金、交通、能源等成本，极大提升运营管理效率，预计到2020年，每年将创造数千亿元经济效益。

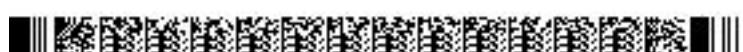
项目研究不仅能够支撑各类互联网应用并通过应用实现降低能源消耗，项目本身的技术研究也强调绿色环保理念，在实现物联网与智慧城市安全体系架构与关键技术的同时，强调技术与系统设计实现的轻量化，低功耗，减少能源消耗，促进人与自然和谐发展。



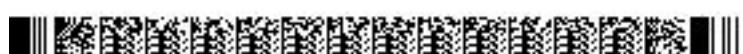
六、项目年度计划

按年度制定完成项目的计划进度，应将项目的考核指标分解落实到年度计划中。

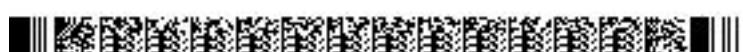
年度	任务	考核指标	成果形式
2018 年 7月 2018 年 12月	<ol style="list-style-type: none">研究安全体系架构中的共性安全技术无打扰的设备发现技术调研基于多元特征的多类型可靠标识生成设备选型及技术；研究基于标识的异构通信协议的选型及兼容性论证多因子情境识别感知技术；基于轻量级加密的数据存储机制；基于功能加密的数据计算机制；基于PUF、物理指纹的轻量级认证技术；多态流量伪装技术确定课题五总体管理、协调及运行、实施机制；确定课题总体及各课题研究方案及工作计划	<ol style="list-style-type: none">发表论文不少于3篇，申请发明专利不少于4项完成基于标识的安全物联网互联互通架构方案设计完成无打扰的设备发现方案设计完成物联网标识生成原型系统的体系架构方案设计；完成物联网协议兼容框架方案设计完成情境识别感知方案设计；撰写国家发明专利申请文档1项	论文、专利、设计方案报告



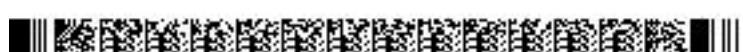
2019年1月 2019年6月	<p>1. 研究原型平台中的感知层平台支撑技术；研究智慧城市安全保障架构的基础设施安全技术</p> <p>2. 跨网跨域的设备快速发现技术</p> <p>3. 调研基于标识的轻量级域内及跨域身份认证技术；研究基于区块链技术的异构标识对等跨域解析机制</p> <p>4. 多因子情境识别感知技术；基于轻量级加密的数据存储机制；基于功能加密的数据计算机制；基于差分隐私的感知数据汇聚处理机制；基于PUF、物理指纹的轻量级认证技术；多模态流量伪装技术</p> <p>5. 文献调研和归纳：跨域服务和分布式信任问题研究。完善实施计划</p>	<p>1. 发表论文不少于4篇，申请发明专利不少于4项</p> <p>2. 完成物联网安全体系架构方案设计；完成智慧城市安全保障技术架构方案设计</p> <p>3. 完成跨网跨域的设备快速发现方案设计</p> <p>4. 初步完成轻量级域内及跨域认证方案设计</p> <p>5. 节点认证支持认证节点种类≥ 5种；</p>	论文、专利、设计方案报告
-------------------	--	---	--------------



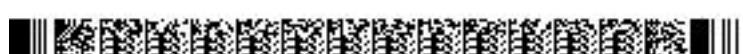
2019 年 7月 2019 年 12月	<p>1. 研究安全体系架构中的共性安全技术、感知层与网络层技术；研究原型平台中的感知层、网络层平台支撑技术</p> <p>2. 基于蜜罐和 IP 溯源的设备行为智能感知</p> <p>3. 研究基于多元特征的多类型可靠标识生成技术及方法；研究基于标识的异构通信协议安全数据路由技术</p> <p>4. 多因子情境识别感知技术；安全异构数据融合技术；基于轻量级加密的数据存储机制；基于功能加密的数据计算机制；基于差分隐私的感知数据汇聚处理机制；基于 PUF、物理指纹的轻量级认证技术；多模态流量伪装技术；基于标识的大规模密钥管理机制</p>	<p>1. 发表论文不少于 5 篇，申请发明专利不少于 4 项</p> <p>2. 完成安全物联网原型平台方案设计</p> <p>3. 完成基于蜜罐和 IP 溯源的设备行为智能感知方案设计</p> <p>4. 初步完成物联网标识生成原型系统；初步完成基于标识的异构通信安全数据路由方案设计</p> <p>5. 设计解决方案，为感知数据存储和计算提供轻量级 / 功能加密服务；节点认证支持认证节点种类 ≥ 15 种；撰写国家发明专利申请文档 1 项</p> <p>6. 完成跨服务域的密钥管理设计方案</p> <p>7. 完成年度技术报告</p>	论文、专利 系统演示平台、 设计方案、原型 系统
--	--	--	-----------------------------------



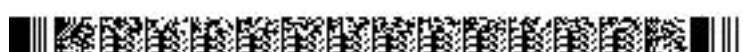
	5. 研究复杂服务域下密钥管理服务的问题		
2020 年 1月 2020 年 6月	<p>1. 研究原型平台中的感知层、网络层平台支撑技术；研究智慧城市安全保障架构的基础设施安全技术、安全管理平台</p> <p>2. 设备特征自动化提取技术；物联网安全子平台</p> <p>3. 调研基于标识的轻量级域内及跨域隐私保护技术；研究异构标识的高效安全分层管理和跨域安全解析技术</p> <p>4. 多因子情境识别感知技术；安全异构数据融合技术；基于差分隐私的感知数据汇聚处理机制；基于 PUF、物理指纹的轻量级认证技术；多模态流量伪装技术；基于低延迟加密的数据传输技术；</p>	<p>1. 发表论文不少于 4 篇，申请发明专利不少于 8 项</p> <p>2. 完成智慧小区和家庭安全原型系统方案设计；完成三类典型应用的方案设计</p> <p>3. 完成设备自动化特征提取方案设计；完成原型系统设计</p> <p>4. 初步完成轻量级域内及跨域隐私保护方案设计(支持隐私数据类型 8 种以上)</p> <p>5. 情境识别感知准确率\geq85%；终端节点认证的错误接受率\leq10%、错误拒绝率\leq5%</p> <p>6. 完成跨服务域强隔离的设计方案；完成授权策略映射的设计方案；</p>	论文、专利 系统演示平台、 设计方案报告



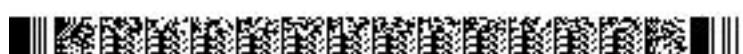
	<p>基于标识的大规模密钥管理机制；面向大连接、时延复杂的云端融合机制；面向节点资源受限的传算结合机制。</p> <p>5. 研究跨服务域的强逻辑隔离；研究基于身份和基于角色的授权策略映射</p>		
中期考核	<p>1. 完成基于标识的安全物联网互联互通架构；物联网安全体系架构；智慧城市安全保障技术架构三个方面的方案设计；完成安全物联网原型平台的方案设计；完成支持智慧城市统一管理的安全控制中心、安全网关、智能防火墙等原型系统的方案设计；完成示范应用的防护体系详细设计</p> <p>2. 无打扰的设备发现技术、跨网跨域的设备快速发现技术、物联网安全</p>	<p>1. 基于标识的安全物联网互联互通架构；物联网安全体系架构；智慧城市安全保障技术架构三个方案设计报告；安全物联网原型平台的方案设计报告；支持智慧城市统一管理的安全控制中心、安全网关、智能防火墙等原型系统的方案设计报告；智慧城市基础地理空间系统、智慧城市大数据中心、智慧能源、智慧物流、智慧交通、智慧城市运营管理中心、智慧教育、智慧社区与家庭八个示范应用的防护体系详细设计报告</p> <p>2. 支持 5 亿规模的设备发现；识别设备的种类$\geqslant 10$ 种，数量支持 5 亿规模；识别准确率不低于 80%；支持 5</p>	中期执行情况报告



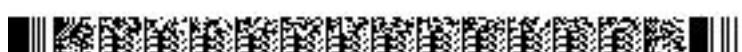
	<p>子平台</p> <p>3. 多因子情境识别感知技术；安全异构数据融合技术；基于轻量级加密的数据存储机制；基于功能加密的数据计算机制；基于差分隐私的感知数据汇聚处理机制；基于 PUF、物理指纹的轻量级认证技术；多模态流量伪装技术；基于标识的大规模密钥管理机制；面向大连接、时延复杂的云端融合机制；面向节点资源受限的传算结合机制</p> <p>4. 完成跨服务域的密钥管理设计方案；完成跨服务域强隔离的设计方案；完成授权策略映射的设计方案</p>	<p>亿规模的设备安全状态探测；不少于 3 种僵尸节点检测能力，数量不少于 6 万；</p> <p>3. 设计解决方案，为感知数据存储和计算提供轻量级/功能加密服务；情境识别感知准确率 $\geq 85\%$；节点认证支持认证节点种类 ≥ 15 种，终端节点认证的错误接受率 $\leq 10\%$、错误拒绝率 $\leq 5\%$</p> <p>4. 高水平论文 ≥ 11 篇</p> <p>5. 申请发明专利 ≥ 20 项</p>	
2020 年 7 月	<p>1. 研究安全体系架构中的感知层与网络层技术、存储层与服务层架构；</p>	<p>1. 发表论文不少于 5 篇，申请发明专利不少于 5 项</p> <p>2. 完成基于标识的安全物联网互联互通架构原型系统</p>	<p>论文、专利 系统演示平台、 实验装置（支持 通信协议及路由</p>



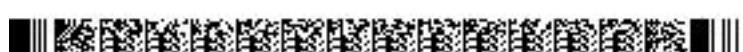
 2020 年 12月	<p>研究原型平台中的网络层、应用层平台支撑技术</p> <p>2. 多维融合的设备识别模型</p> <p>3. 研究基于标识的轻量级域内及跨域身份认证和数据隐私保护技术及方法；研究支持多种物联网通信协议和路由协议的网络融合方案</p> <p>4. 安全异构数据融合技术；基于差分隐私的感知数据汇聚处理机制；多模态流量伪装技术；基于低延迟加密的数据传输技术；基于标识的大规模密钥管理机制；面向大连接、时延复杂的云端融合机制；面向节点资源受限的传算结合机制</p> <p>5. 研究复杂服务域下安全协商机制的原型系统的建立及其应用场景和性能</p>	<p>3. 完成基于标识的安全物联网跨域认证及隐私保护方案（支持异构标识不少于3种）；完成互联互通协议融合的实验装置</p> <p>4. 完成虚假数据检测方案设计；完成数据和通信隐私保护方案设计；撰写国家发明专利申请文档1项</p> <p>5. 完成跨服务域的强逻辑隔离系统的搭建</p> <p>6. 完成年度技术报告</p>	协议均不少于4种）、设计方案报告
----------------------	---	---	------------------



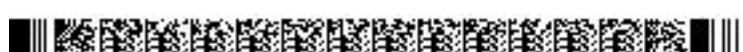
<p>2021 年 1月 2021 年 6月</p>	<ol style="list-style-type: none"> 1. 研究原型平台中的网络层、应用层平台支撑技术；研究智慧城市安全保障架构的安全管理平台、应用与数据安全 2. 设备快速识别技术、设备状态主动探测与模糊推断、基于蜜罐和 IP 溯源的设备行为智能感知、多维融合的设备识别模型 3. 调研 DHT 技术，研究异构标识的高效安全分层管理和跨域安全解析技术；研究基于标识的跨域多维分级授权和访问控制的协议架构 4. 安全异构数据融合技术；基于差分隐私的感知数据汇聚处理机制；多模态流量伪装技术；基于低延迟加密的数据传输技术；基于标识的大规模密钥管理机制；面向大连接、时延复杂的云端 	<ol style="list-style-type: none"> 1. 发表论文不少于 7 篇，申请发明专利不少于 5 项 2. 完成物联网安全体系架构原型系统；完成智慧城市安全保障技术架构原型系统 3. 完成设备快速识别方案设计；完成设备状态主动探测与模糊推断以及基于蜜罐和 IP 溯源的设备行为智能感知的方案设计；提出多维融合的设备识别模型 4. 完成异构标识安全分层管理和跨域解析方案；完成跨域多维分级授权和访问控制的协议架构方案 5. 虚假数据检测准确率\geq90%；数据隐私保护针对可量化的数据查询，数据差分隐私预算≤ 1，数据噪声比$\leq 5\%$或查询结果误差$\leq 5\%$；通信隐私保护可抵御基于流量分析的侧信道攻击；设计解决方案，为延迟敏感应用提供低延迟加密服务 6. 完成支持 10 亿规模的密钥管理服务系统的搭建；完成授权策略映射系统的搭建； 	<p>论文、专利 系统演示平台、 设计方案报告</p>
--	--	---	-------------------------------------



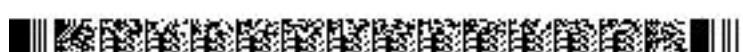
	<p>融合机制；面向节点资源受限的传算结合机制</p> <p>5. 研究复杂服务域下安全协商机制的原型系统的建立及其应用场景和性能</p>		
2021 年 7月 2021 年 12月	<p>1. 完成三类典型应用的示范演示工作, 在典型场景下验证所提出的机制和算法;</p> <p>2. 主被动结合的物联网设备发现技术、安全可靠的物联网数据采集感知</p> <p>3. 调研 DHT 技术, 研究异构标识的高效安全分层管理和跨域安全解析技术; 研究基于标识的跨域多维分级授权和访问控制的协议架构</p> <p>4. 研究基于标识的跨域多维分级授权; 研究基于标识的跨域访问控制机制; 完成课题三个子课题的方</p>	<p>1. 发表论文不少于 8 篇, 申请发明专利不少于 5 项</p> <p>2. 完善关键算法, 解决系统设计和开发的问题, 准备验收; 进行课题的测试、总结, 验收和演示</p> <p>3. 完成主被动结合的物联网设备发现以及安全可靠的物联网数据采集感知方案设计</p> <p>4. 实现多维分级授权功能验证; 完成跨域多维分级授权和访问控制机制的方案设计(包含 4 个管理域)</p> <p>5. 完成云端融合和传算结合设计方案</p> <p>6. 完成原型系统的集成和联调; 跨服务域强隔离通过国家主管部门安全审查; 原型系统的 10 亿规模的密钥管理和授权管理映射不大于 1 分钟通过第三方测评</p>	<p>论文、专利 系统演示平台、 设计方案报告、 专家鉴定意见报 告</p>



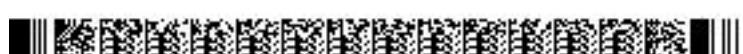
	<p>案的融合及论证</p> <p>5. 面向大连接、时延复杂的云端融合机制；面向节点资源受限的传算结合机制</p> <p>6. 完成动态跨域的大规模分布式安全信任机制与管理系统，并进行试点部署</p>	<p>7. 完成年度技术报告</p>	
2022 年 1月 2022 年 6月	<p>1. 完成安全应用部署和 测试，优化 系统，对验收 指标进行评价和验 证</p> <p>2. 物联网安全子平 台</p> <p>3. 继续完善课题三 研究内容，继续完 善系统设计和开 发的问题，准备验 收；进行课题的整 体测试、总结、验 收和论证</p> <p>4. 面向大连接、时延 复杂的云端融合 机制；面向节点资 源受限的传算结 合机制。</p>	<p>1. 发表论文不少于 3 篇，申请 发明专利不少于 2 项</p> <p>2. 完成安全物联网原型平 台；完成智慧小区和家庭 安全原型系统；完成三类 典型应用示范</p> <p>3. 实现无代理的物联网设备 发现，支持 10 亿规模设备 发现；识别设备的种类≥ 15 种，包括但不限于摄像 头、打印机、路由器、PLC、 RTU、SCADA、智能开关、 智能照明、智能穿戴等； 数量支持 10 亿规模；识别 准确率不低于 95%；实现物 联网设备状态的智能推 断，支持 10 亿规模；不少 于 5 种僵尸网络物联网节 点检测能力，总体僵尸节</p>	论文、专利 系统演示平台、 标准



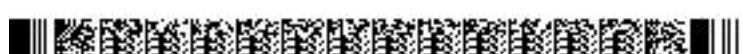
	<p>5. 完成动态跨域的大规模分布式安全信任机制与管理系统，并进行试点部署</p>	<p>点数量不少于 10 万。</p> <p>4. 完成课题 3 的整体系统架构；关键技术集成到智慧小区和家庭安全原型系统</p> <p>5. 标准（送审稿）3 项</p> <p>6. 完成原型系统的搭建与试点的部署</p>	
课题验收 (2022 年 6 月)	<p>1. 完成基于标识的安全物联网互联互通架构；物联网安全体系架构；智慧城市安全保障技术架构；完成安全物联网原型平台；完成支持智慧城市统一管理的安全控制中心、安全网关、智能防火墙等原型系统；完成三类八个典型示范应用的防护体系</p> <p>2. 无安全代理的物联网设备发现技术；多维属性融合的设备识别模型及方法；设备安全状态探测与行为智能推断方法；指标 2.4 物联网安全</p>	<p>1. 完成用于安全体系架构验证的硬件设备及软件系统的支持平台。平台至少支持 2 种国密算法、支持至少 3 种安全通信协议、研发至少 3 种安全测试终端。</p> <p>防火墙吞吐量 240 Gbps，安全网关，最大并发连接数 1800，安全控制中心新建连接速率 160 万/秒；内网工作站具有加密和外设管理功能；内网服务器具有可信程序管理功能；具有内外网摆渡区安全防护功能；外网工作站具有外设管理功能和多模透明加密功能；外网移动工作站具有离线安全管理功能。;</p> <p>实现示范应用的等保三级，至少一个地级市示范；包含入侵检测安全技术、安全审计、防火墙、抵抗拒绝服务攻击、网络防病毒系统、流量整形和控制、</p>	结题验收情况报告



	<p>监控子平台</p> <p>3. 多因子情境识别感知技术；安全异构数据融合技术；基于轻量级加密的数据存储机制；基于功能加密的数据计算机制；基于差分隐私的感知数据汇聚处理机制；基于 PUF、物理指纹的轻量级认证技术；多模态流量伪装技术；基于低延迟加密的数据传输技术；基于标识的大规模密钥管理机制；面向大连接、时延复杂的云端融合机制；面向节点资源受限的传算结合机制</p>	<p>加密技术和使用识别管理等功能；示范应用至少在五个小区示范；具有用户隐私保护和电子支付安全防护等功能</p> <p>2. 实现无代理的物联网设备发现，支持 10 亿规模设备发现；识别设备的种类≥15 种，包括但不限于摄像头、打印机、路由器、PLC、RTU、SCADA、智能开关、智能照明、智能穿戴等；数量支持 10 亿规模；识别准确率不低于 95%；实现物联网设备状态的智能推断，支持 10 亿规模；不少于 5 种僵尸网络物联网节点检测能力，总体僵尸节点数量不少于 10 万</p> <p>3. 支持设备种类不少于 10 种（如 RFID 标签、二维码标签、摄像头标识等），设备标识的生成特征不少于 5 种（如标识物理状态、感知状态、安全状态等）；支持物联网通信协议不少于 4 种（如 NB-IOT，LoRa，蓝牙，wifi，zigbee）、路由协议不少于 4 种（AODV、LEACH、SPIN、SEIF 等）；支持异构标识种类 3 种以上（RFID、二维码、条形码等等），支持隐私数据类型 8 种以上（位置、时钟、属主等）；支持异构标识种类 3 种以上（RFID、二维码、条形码等等）；管理域数量 4(管理域一-Zigbee 无线网络协调器管理域；管理域二-网关管理域；管理域三-本地或远程服务器管理域；管理域四-云存</p>	
--	--	---	--



	<p>储服务管理域), 身份数量 15 (身份即节点标识, 即节点标识数量 15), 角色数量 4 (源节点角色、目的节点角色、网关管理节点角色、云存储服务角色); 实现多维分级授权功能验证</p> <p>4. 情境识别感知准确率 $\geq 85\%$; 虚假数据检测准确率 $\geq 90\%$; 认证节点种类 ≥ 15 种, 终端节点认证的错误接受率 $\leq 10\%$、错误拒绝率 $\leq 5\%$; 数据隐私保护针对可量化的数据查询, 数据差分隐私预算 ≤ 1, 数据噪声比 $\leq 5\%$ 或查询结果误差 $\leq 5\%$; 通信隐私保护可抵御基于流量分析的侧信道攻击; 设计解决方案, 为延迟敏感应用提供低延迟加密服务, 为感知数据存储和计算提供相应的加密服务;</p> <p>5. 完成原型系统的搭建与试点的部署; 原型系统的跨服务域强隔离通过国家主管部门安全审查; 原型系统的 10 亿规模的密钥管理和授权管理映射不大于 1 分钟通过第三方测评</p> <p>6. 包括上面指标中的成果, 标准 (送审稿) 3 项, 发表论文 ≥ 38 篇, 其中高水平论文 ≥ 20 篇, 申请发明专利 ≥ 36 项</p>	
--	--	--



七、项目组织实施机制及保障措施

1、项目及各任务（课题）的内部组织管理方式、协调机制等，限 1000 字以内。

1.1 项目整体的组织管理方式

项目总体组和办公室根据项目整体研究目标制定组织管理方式，对课题进行统一管理，协调研究工作进度，建立共同责任和风险应对机制，保障完成各项研究目标。

项目专家组与项目管理团队相结合，及时发现、协调和解决出现的各种问题，对研究工作的技术方向、成果水平和整体进度进行有效的管理。

项目总体组、办公室与各课题组配合，制定严格的项目研究成果接口管理规范，各课题组提供课题之间的接口设计方案和验证方案，确保各课题研究工作的一致性和项目工作的完整性。

1.2 各课题内部的组织管理方式

项目内部各课题确定课题接口人，保障各课题之间、各课题与项目办公室的信息交流，及时报告研究进展和问题解决进度。

各课题内部根据课题研究目标和年度研究任务，确定子课题工作组。各课题负责人定期检查子课题的研究进展，并按月汇总子课题的研究进展、后续研究计划以及出现的问题和解决方案，完成课题研究工作简报并提交项目办公室，保障项目的统筹协调推进。

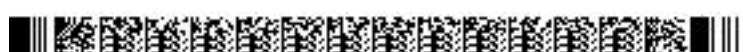
1.3 周期性的会议协调机制

本项目每半年召开一次科研进展工作会议，参加人员包括：五个课题的课题组长和科研骨干、项目首席科学家、项目咨询专家组，以及项目申报单位的科研管理部门负责人。主要听取项目的总体进展汇报、各个课题的科研进展报告，以及项目的财务支出情况报告。项目咨询专家组对各个课题的进展情况进行评估，对共性问题提出解决思路和建议。

2、项目实施的相关政策，已有的组织、技术基础，支撑保障条件，限 1000 字以内。

2.1 政策法规支撑条件

《国家中长期科学和技术发展规划纲要（2006—2020 年）》中“下一代网络关键技术与服务”的优先主题中明确提出建立可信的网络管理体系。因此聚焦网络安全紧迫技术需求和重大科学问题，突破基础理论和关键技术，推动建立与国际同步、并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迫在眉睫。科技部、工信部、自然科



学基金委等通过相关计划项目对网络安全体系结构技术研发、应用示范、服务推广进行了广泛支持，提供了良好的政策保障。

2.2 组织支撑条件

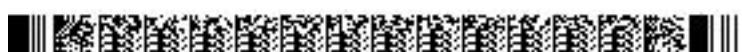
高效的项目组织能够保障研究工作的顺利进行。项目依托中国科学技术大学作为项目牵头单位，联合清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司等国内一流的研究机构与企业，在物联网体系结构、网络空间安全、无线网络、智慧城市建设等领域已具备坚实的研究基础，取得了一批国际领先水平的学术成果，多次获得国家科技奖励和国际学术奖励。同时，本项目各单位长期开展合作研究，共同承担和完成了多项国家973、863、下一代互联网专项等国家级科研项目，具有长期的合作基础和丰富的组织管理经验，为项目的顺利开展和实施奠定了坚实的基础、提供了有力的组织保障。

2.3 资源支撑条件

中国科学技术大学具有大规模物联网的示范平台，与国内高校和企业在物联网标准化、产业联盟方面有广泛合作。参与项目的各个单位在网络安全协议开发和平台建设方面具有良好的工作基础。其中，中国科学技术大学、清华大学和东南大学具备国内外少有的大规模IPv6网络试验环境和试验用户群体，为项目顺利开展提供了良好的资源保障。

3、对实现专项总目标的支撑作用，及与专项内其他相关项目的协同机制，限1000字以内。

本项目的主要研究内容是研发物联网与智慧城市共性安全关键技术，构建适应智慧城市与物联网安全目标的模型和体系框架，研制安全物联网原型平台，构建智慧小区和智慧家庭的应用示范系统。支持分级分层管理与安全解析，物联网设备发现、识别和监控以及身份认证、密钥管理服务均支持10亿规模；设计完成采用国家标准密码算法的物联网管理域的强逻辑隔离安全机制；支持基于身份和角色的授权策略映射，支持时间、环境以及安全上下文敏感的授权管理；开发完成支持智慧城市统一管理的安全控制中心、安全网关、智能防火墙等原型系统，并通过权威部门测评，得到试点应用；起草制



定相关国际、国家或行业标准；实施不少于 5 个小区、3 类智慧家庭、智慧小区、智慧城市典型应用示范。

对专项总目标的支撑作用主要体现在以下几个方面：

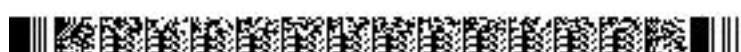
(1) 通过构建适应智慧城市与物联网安全目标的模型和体系框架，研制安全物联网原型平台，构建智慧小区和智慧家庭的应用示范系统，为实现专项总体目标中“聚焦网络安全紧迫技术需求和重大科学问题，坚持开放发展，着力突破网络空间安全基础理论和关键技术，研发一批关键技术装备和系统，逐步推动建立起与国际同步，适应我国网络空间发展的、自主网络空间安全保护技术体系、网络空间安全治理技术体系和网络空间测评分析技术体系”等方面提供理论模型支撑。

(2) 通过突破动态跨域的大规模分布式信任服务机理，大连接复杂异构条件下的物联网一体化安全机制，基于异构标识的安全物联网互联互通机制与协议以及无安全代理的大规模设备智能发现、感知和监控这四项关键技术，解决“资源受限的智能感知标识”、“大规模泛在网络的安全异质互联”、“复杂跨域环境下的信任机理”三个关键科学问题。为实现专项总体目标提供技术支撑及平台支撑。

(3) 本项目同专项内其他项目间可根据技术体系、以及示范应用的相关程度进行有效地协同，共同推进整个专项的顺利实施，具体的协同关系如下：

a) 对于指南方向 2，对于开放融合环境下的数据安全保护理论与关键技术研究中，本项目从技术上能够对指南 2.1 移动互联网数据防护技术试点示范提供技术保障，同时也为相关项目中关键技术在具体行业中的应用示范提供借鉴和参考。

b) 对于指南方向 3 网络空间数字资产保护创新方法与关键技术研究中，3.1 互联网+环境中基于国产密码的多媒体版权保护与监管技术，以及 3.3 支持全程电子化的电子发票及服务系统试点示范，项目能够结合共性关键技术提供理论框架指导及平台支撑。



八、知识产权对策、成果管理及合作权益分配

项目联合参加单位本着相互合作的精神，对项目申请和执行过程中涉及的知识产权归属、成果管理、合作权益分配按以下方式处理：

1、项目联合参加单位在申请本项目之前对各自所获得的知识产权及相应权益均归各自所有，不因共同申请本项目而改变。

2、因申请项目的需要，各自向对方提供的未公开的、或在提供之前已告知不能向第三方提供的与本项目相关的技术资料、数据等所有信息，包括但不限于各自所有或合法拥有的任何计算机程序、代码、算法、公式、过程、观念、图表、照片、制图、设计、产品、样品、发明创造（包括发明、实用新型和外观设计，无论是否获得专利）、技术秘密、版权、商标、产品研发计划、预测、策略、规范、实际或潜在商业活动的信息、客户与供应商名单、财务事项、市场营销计划等技术、商务上的信息等。未经提供方同意，不得提供给第三方。

3、因申请本项目的需要，各自向对方提供的相关信息，不构成向对方授予任何关于专利、著作权、商标权等知识产权的许可行为。

4、在项目执行过程中，各方对项目执行过程中产生的科技成果按下列方式及时采取知识产权保护措施：

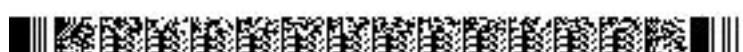
(1) 根据项目任务分工，在各方的工作范围内独立完成的科技成果及其形成的知识产权归各方独自所有。一方转让其专利申请权时，其他各方有以同等条件优先受让的权利。

(2) 在项目执行过程中，由各方共同完成的科技成果及其形成的知识产权归各方共有。一方转让其共有的专利申请权的，其他各方有以同等条件优先受让的权利。一方声明放弃其共有的专利申请权的，可以由另一方单独申请或者由其他各方共同申请。合作各方中有一方不同意申请专利的，另一方或其他各方不得申请专利。

(3) 由各方共同完成的技术秘密成果，各方均有独自使用的权利。未经其他各方同意，任何一方不得向第三方转让技术秘密。

(4) 共同完成的科技成果的精神权利，如身份权、依法取得荣誉称号、奖章、奖励证书和奖金等荣誉权归完成方共有。

(5) 各方对共有科技成果实施许可、转让专利技术、非专利技术而获得的经济收益由各方共享。收益共享方式应在行为实施前另行约定。



九、需要约定的其他内容

第一条 甲方有权根据项目年度财政预算批复、立项前期情况、计划进度完成情况、资金使用情况等确定经费拨付安排。

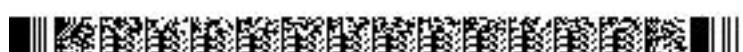
第二条 乙方应积极配合甲方开展监督、检查、评估等过程管理工作，应每 6 个月向甲方报告项目执行情况及下 6 个月工作计划，项目实施关键节点的重大会议、活动应邀请甲方和责任专家参加。

第三条 对于同一指南方向拟支持 1-2 项并确定支持 2 项的项目，甲方将组织项目中期评估，并根据评估结果确定后续支持方式。

第四条 根据甲方需要，乙方应配合做好信用评价、绩效评价、里程碑实施计划及其他项目管理相关工作。

第五条 任务书履行期间，若国家颁布新的科技计划相关管理规定，甲乙双方按新颁布的相关管理规定执行。

第六条 项目未完成任务目标，任务验收结论为结题或不通过的，项目下所有课题结余资金由项目牵头单位统一组织上交专业机构。

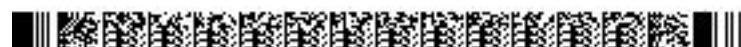


十、项目参加人员基本情况表

填表说明:

1. 职称分类: A、正高级 B、副高级 C、中级 D、初级 E、其他;
2. 投入本项目的全时工作时间(人月)是指在项目实施期间该人总共为项目工作的满月度工作量; 累计是指项目组所有人员投入人月之和;
3. 项目固定研究人员需填写人员明细;
4. 是否有工资性收入: Y、是 N、否;
5. 人员分类代码: A、项目负责人 B、任务(课题)负责人 C、项目骨干 D、其他研究人员;
6. 工作单位: 填写单位全称, 其中高校要具体填写到所在院系。

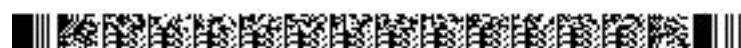
序号	姓名	性别	出生日期	身份证号码 (军官证、护照)	技术职称	职务	学位	专业	投入本项目的 全时工作时间 (人月)	人员分类	所属任务 (课题)	是否有 工资性 收入	工作单位	参加人员 签字
1	李向阳	男	1971-10-28	321025197110282833	正高级	院长	博士	计算机软件与理论	24	项目负责人	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	中国科学技术大学计算机科学与技术学院	
2	姜建国	男	1964-01-02	510702196401029356	正高级	无	博士	信息安全	24	任务(课题)负责人	无安全代理的大规模设备智能发现、感知和监控	Y	中国科学院信息工程研究所第四研究室	



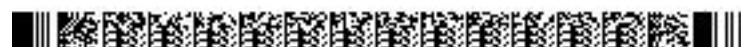
3	肖甫	男	1980-10-05	321102198010050459	正高级	副院长	博士	计算机应用技术	40	任务(课题)负责人	基于异构标识的安全物联网互联互通机制与协议	Y	南京邮电大学 计算机学院、软件学院、网络空间安全学院	
4	杨明	男	1979-02-02	320402197902022534	副高级	无	博士	计算机网络	28	任务(课题)负责人	大连接复杂异构条件下的物联网一体化安全机制	Y	东南大学计算机科学与工程学院	
5	徐恪	男	1974-12-09	110108197412098918	正高级	教授	博士	计算机科学与技术	24	任务(课题)负责人	动态跨域的大规模分布式信任服务机理	Y	清华大学计算机科学与技术系	
6	李义常	男	1989-12-08	422201198912080810	中级	无	博士	物联网	24	项目骨干	适应智慧城市与物联网安全目标的	Y	中国科学技术大学计算机科学与技术学院	



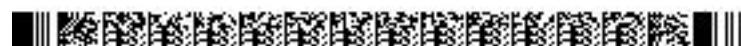
										安全架构和 应用示范			
7	何昕	男	1986-10-19	340827198610193216	中级	无	博士	通信工程	24	项目骨干	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	中国科学技术大学计算机科学与技术学院
8	李强	男	1973-06-21	210106197306213813	副高级	技术总监	硕士	计算机应用	20	项目骨干	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	北京奇安信科技有限公司
9	吴亚东	男	1974-01-10	350426197401100019	中级	系统架构师	学士	国际贸易	32	项目骨干	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	北京奇安信科技有限公司



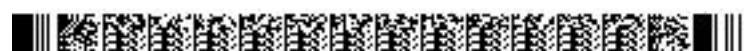
10	刘洪亮	男	1977-01-03	220104197701034419	中级	技术总监	硕士	计算机应用	20	项目骨干	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	北京奇安信科技有限公司	
11	王伟	男	1978-02-12	131082197802120511	中级	副总裁	学士	化学工程与工艺	20	项目骨干	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	北京奇安信科技有限公司	
12	张延强	男	1982-03-07	410721198203073510	副高级	无	博士	信号与信息处理	40	项目骨干	适应智慧城市与物联网安全目标的安全架构和应用示范	N	国家信息中心 信息化和产业发展部	
13	肖青	男	1979-12-06	22010419791206153X	副高级	总经理	硕士	微电子与固体电子学	40	项目骨干	适应智慧城市与物联网	Y	中移物联网有限公司	



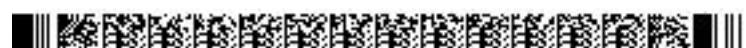
										安全目标的 安全架构和 应用示范			
14	马萃林	男	1982-02-24	110105198202240811	其他	射频开发高 级工程师	学士	通信工程	40	项目骨干	适应智慧城市与物联网 安全目标的 安全架构和 应用示范	Y	中移物联网有 限公司
15	王雷	男	1986-09-13	321324198609134033	其他	嵌入式软件 开发高级工 程师	学士	自动化	40	项目骨干	适应智慧城市与物联网 安全目标的 安全架构和 应用示范	Y	中移物联网有 限公司
16	李宁	男	1983-09-09	110223198309093119	其他	产品经理	硕士	软件项目管 理	48	项目骨干	适应智慧城市与物联网 安全目标的 安全架构和	Y	中移物联网有 限公司



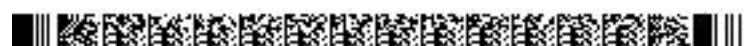
17	马益荣	女	1978-02-23	37108219780223162X	副高级	总监	学士	劳动经济/ 人力资源管 理	24	项目骨干	适应智慧城市与物联网安全目标的 安全架构和应用示范	Y	北京泰豪智能工程有限公司
18	李强	男	1986-07-07	330324198607072116	中级	讲师	博士	计算机网络	24	项目骨干	无安全代理 的大规模设 备智能发 现、感知和 监控	Y	北京交通大学 计算机与信息 技术学院
19	陈永乐	男	1983-08-07	370781198308076033	副高级	无	博士	信息安全	24	项目骨干	无安全代理 的大规模设 备智能发 现、感知和 监控	Y	太原理工大学 计算机科学与 技术学院
20	刘伟	男	1985-09-21	370306198509211519	副高级	无	博士	信息安全	24	项目骨干	无安全代理	Y	北京富邦智慧



										的大规模设备智能发现、感知和监控		物联科技有限公司	
21	周颢	男	1976-01-28	42060119760128001X	副高级	无	博士	计算机科学与技术	24	项目骨干	无安全代理的大规模设备智能发现、感知和监控	Y	中国科学技术大学计算机科学与技术学院
22	曹志超	男	1987-08-29	130503198708290333	中级	助理研究员	博士	计算机科学与技术	40	项目骨干	基于异构标识的安全物联网互联互通机制与协议	Y	清华大学软件学院
23	陈红松	男	1977-10-16	370802197710164512	副高级	副教授	博士	计算机科学与技术	32	项目骨干	基于异构标识的安全物联网互联互通机制与协议	Y	北京科技大学计算机与通信工程学院



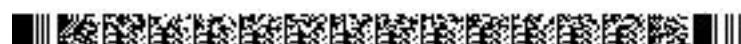
										通机制与协 议			
24	谷雨	男	1986-01-04	342622198601044875	正高级	教授	博士	计算机	24	项目骨干	基于异构标 识的安全物 联网互联互 通机制与协 议	Y	合肥工业大学 计算机与信息 学院
25	田野	男	1979-06-17	510214197906171799	副高级	副研究员	博士	物联网	24	项目骨干	基于异构标 识的安全物 联网互联互 通机制与协 议	Y	中国科学院计 算机网络信息 中心物联网信 息技术与应用 实验室
26	丁旋	男	1986-06-17	429006198606175835	中级	助理研究员	博士	计算机网络	40	项目骨干	基于异构标 识的安全物 联网互联互 通机制与协 议	Y	清华大学软件 学院



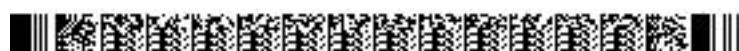
27	宋爱波	男	1969-02-03	370628196902037911	正高级	无	博士	计算机网络	28	项目骨干	大连接复杂异构条件下的物联网一体化安全机制	Y	东南大学计算机科学与工程学院	
28	凌振	男	1982-01-30	320223198201300410	副高级	无	博士	计算机网络	32	项目骨干	大连接复杂异构条件下的物联网一体化安全机制	Y	东南大学计算机科学与工程学院	
29	吴文甲	男	1983-11-21	32090219831121005X	副高级	无	博士	计算机网络	32	项目骨干	大连接复杂异构条件下的物联网一体化安全机制	Y	东南大学计算机科学与工程学院	
30	刘云淮	男	1977-05-31	110108197705316333	正高级	公共安全大数据研究室	博士	计算机科学与技术	24	项目骨干	大连接复杂异构条件下	Y	北京大学前沿交叉研究院	



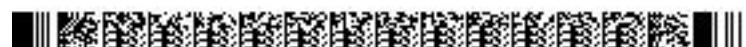
					主任				的物联网一 体化安全机 制			
31	杨元元	女	1956-10-23	453871209	正高级	IEEE Transactio ns on Computers 副主编	博士	计算机科学 与技术	40	项目骨干	大连接复杂 异构条件下 的物联网一 体化安全机 制	Y
32	郭松涛	男	1975-12-18	510212197512180331	正高级	副院长	博士	计算机科学 与技术	40	项目骨干	大连接复杂 异构条件下 的物联网一 体化安全机 制	Y
33	杨阳	男	1982-03-07	510421198203070018	副高级	无	硕士	计算机科学 与技术	32	项目骨干	大连接复杂 异构条件下 的物联网一 体化安全机 制	Y



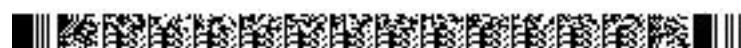
34	肖国玉	男	1968-12-16	32072219681216777x	正高级	执行董事	博士	网络数据安全、数据分析	40	项目骨干	大连接复杂异构条件下 的物联网一体化安全机制	Y	上海汉邦京泰数码技术有限公司
35	李丹丹	女	1981-09-13	330681198109131623	副高级	无	硕士	企业管理	44	项目骨干	大连接复杂异构条件下 的物联网一体化安全机制	Y	上海汉邦京泰数码技术有限公司
36	孙海云	男	1968-09-26	32030319680926165X	副高级	无	学士	计算机科学与技术	40	项目骨干	大连接复杂异构条件下 的物联网一体化安全机制	Y	上海汉邦京泰数码技术有限公司
37	龚莎莎	女	1988-10-31	320323198810311022	副高级	无	学士	计算机网络	44	项目骨干	大连接复杂	Y	上海汉邦京泰



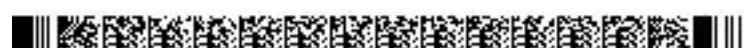
							技术			异构条件下的物联网一体化安全机制		数码技术有限公司	
38	赵玉成	男	1989-09-20	320321198909207038	副高级	无	学士	计算机科学与技术	44	项目骨干	大连接复杂 异构条件下的物联网一体化安全机制	Y	上海汉邦京泰数码技术有限公司
39	夏雷	男	1984-07-10	32030319840710161X	副高级	无	学士	计算机科学与技术	40	项目骨干	大连接复杂 异构条件下的物联网一体化安全机制	Y	上海汉邦京泰数码技术有限公司
40	谈海生	男	1981-09-17	342622198109170431	副高级	无	博士	计算机科学与技术	24	项目骨干	大连接复杂 异构条件下的物联网一	Y	中国科学技术大学计算机科学与技术学院



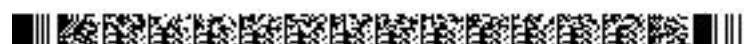
										体化安全机制			
41	于红波	女	1980-02-02	371083198002025546	副高级	副教授	博士	计算机科学与技术	40	项目骨干	动态跨域的大规模分布式信任服务机理	Y	清华大学计算机科学与技术系
42	赵乙	男	1994-03-19	130227199403190031	其他	无	学士	计算机科学与技术	40	项目骨干	动态跨域的大规模分布式信任服务机理	N	清华大学计算机科学与技术系
43	李子巍	男	1988-10-10	110105198810106157	其他	无	硕士	计算机科学与技术	40	项目骨干	动态跨域的大规模分布式信任服务机理	N	清华大学计算机科学与技术系
44	徐磊	男	1983-08-14	632123198308142538	其他	无	学士	计算机科学与技术	40	项目骨干	动态跨域的大规模分布式信任服务	N	清华大学计算机科学与技术系



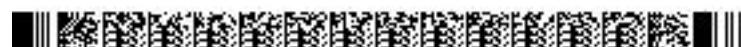
45	李立	女	1983-07-24	14260319830724102X	其他	无	硕士	计算机科学与技术	40	项目骨干	动态跨域的大规模分布式信任服务机理	N	清华大学计算机科学与技术系
46	姚龙	男	1976-01-06	海字第 604480	其他	无	硕士	计算机科学与技术	40	项目骨干	动态跨域的大规模分布式信任服务机理	N	清华大学计算机科学与技术系
47	王晓亮	男	1986-11-09	610481198611090536	其他	无	博士	计算机科学与技术	40	项目骨干	动态跨域的大规模分布式信任服务机理	Y	清华大学计算机科学与技术系
48	阎林	男	1986-08-10	120103198608105811	其他	无	博士	计算机科学与技术	40	项目骨干	动态跨域的大规模分布式信任服务机理	Y	清华大学计算机科学与技术系



49	吕亮	男	1986-04-04	130683198604047336	其他	无	硕士	计算机科学与技术	40	项目骨干	动态跨域的大规模分布式信任服务机理	N	清华大学计算机科学与技术系	
50	苗付友	男	1973-05-10	412801197305102033	副高级	副教授	博士	计算机科学与技术	30	项目骨干	动态跨域的大规模分布式信任服务机理	Y	中国科学技术大学计算机科学与技术学院	
51	黄文超	男	1982-06-07	420503198206075210	副高级	副教授	博士	计算机科学与技术	24	项目骨干	动态跨域的大规模分布式信任服务机理	Y	中国科学技术大学计算机科学与技术学院	
52	王磊	男	1983-10-02	130683198310020373	副高级	副教授	博士	计算机科学与技术	40	项目骨干	动态跨域的大规模分布式信任服务机理	Y	上海交通大学电子信息与电气工程学院、计算机科学与工程系	



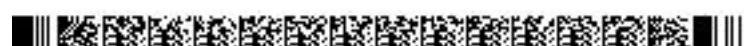
53	甘玉玺	男	1968-11-30	413022196811300416	正高级	总监	硕士	计算机科学与技术	32	项目骨干	动态跨域的大规模分布式信任服务机理	Y	中兴通讯股份有限公司云计算与 IT 经营部	
54	沈蒙	男	1988-01-26	371422198801260015	中级	讲师	博士	计算机科学与技术	40	项目骨干	动态跨域的大规模分布式信任服务机理	Y	北京理工大学计算机学院	
55	郝明亮	男	1988-02-11	13043419880211241X	其他	FAE 高级工程师	学士	应用物理学	40	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	中移物联网有限公司	
56	王新鹏	男	1988-07-16	150428198807160839	其他	硬件开发高级工程师	学士	电子科学与技术（光电方向）	40	其他研究人员	适应智慧城市与物联网安全目标的安全架构和	Y	中移物联网有限公司	



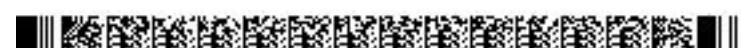
										应用示范			
57	赵志新	男	1986-11-19	110228198611190659	其他	硬件开发工程师	学士	电子信息工程	40	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	中移物联网有限公司
58	汪智慧	男	1984-06-07	421023198406072435	其他	嵌入式软件开发高级工程师	学士	电子信息工程	40	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	中移物联网有限公司
59	张云龙	男	1989-06-15	110111198906151830	其他	嵌入式软件开发高级工程师	学士	信息与计算科学	40	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	中移物联网有限公司
60	史磊	男	1985-12-04	110224198512044431	其他	Java 开发高	学士	机械工程及	48	其他研究	适应智慧城市	Y	中移物联网有



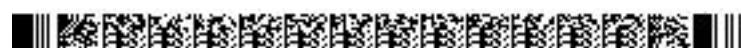
					级工程师		自动化		人员	市与物联网 安全目标的 安全架构和 应用示范		限公司		
61	唐天然	男	1991-07-06	150403199107064835	其他	Java 开发工 程师	学士	电子信息科 学与技术	48	其他研究 人员	适应智慧城 市与物联网 安全目标的 安全架构和 应用示范	Y	中移物联网有 限公司	
62	吕欣	男	1977-01-03	13010219770103211X	正高级	副主任（副 局级）	博士	通信与信息 系统	40	其他研究 人员	适应智慧城 市与物联网 安全目标的 安全架构和 应用示范	N	国家信息中心 办公室	
63	唐斯斯	女	1982-08-20	43052219820820008X	副高级	副处长	博士	经济学	40	其他研究 人员	适应智慧城 市与物联网 安全目标的	N	国家信息中心 信息化和产业 发展部	



										安全架构和 应用示范			
64	马潮江	男	1974-07-12	510322197407124459	正高级	处长	硕士	工商管理	40	其他研究 人员	适应智慧城 市与物联网 安全目标的 安全架构和 应用示范	N	国家信息中心 信息化和产业 发展部
65	吴洁倩	女	1981-04-09	331082198104090169	中级	无	博士	管理科学与 工程	40	其他研究 人员	适应智慧城 市与物联网 安全目标的 安全架构和 应用示范	N	国家信息中心 信息化和产业 发展部
66	李阳	男	1983-02-26	412829198302260010	副高级	无	博士	信息安全	40	其他研究 人员	适应智慧城 市与物联网 安全目标的 安全架构和 应用示范	N	国家信息中心 办公室



67	朱平	男	1970-03-18	612101197003180078	其他	智慧城市副总工	硕士	计算机应用技术	24	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	北京泰豪智能工程有限公司	
68	程志金	男	1986-12-28	371323198612281416	其他	博士后	博士	控制科学与工程	24	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	北京泰豪智能工程有限公司	
69	杜晗	男	1978-11-02	110108197811026831	副高级	智能建筑副总工	硕士	控制工程	24	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	Y	北京泰豪智能工程有限公司	
70	万玮	女	1983-12-03	360102198312031647	中级	智慧城市研究院副院长	硕士	通信与信息	24	其他研究人员	适应智慧城市与物联网	Y	北京泰豪智能工程有限公司	



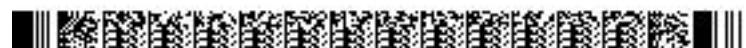
										安全目标的 安全架构和 应用示范			
71	曾凡平	男	1967-05-15	230103196705153256	副高级	无	博士	信息安全	16	其他研究 人员	适应智慧城市与物联网 安全目标的安全架构和 应用示范	Y	中国科学技术 大学计算机科 学与技术学院
72	黄文超	男	1982-06-07	420503198206075210	副高级	副教授	博士	计算机科学 与技术	24	其他研究 人员	适应智慧城市与物联网 安全目标的安全架构和 应用示范	Y	中国科学技术 大学计算机科 学与技术学院
73	卢建良	男	1984-09-22	371426198409222810	中级	无	硕士	计算机科学 与技术	24	其他研究 人员	适应智慧城市与物联网 安全目标的安全架构和	Y	中国科学技术 大学计算机科 学与技术学院



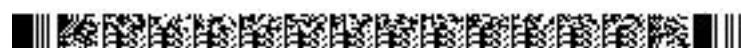
										应用示范			
74	薛爽爽	女	1993-06-19	342221199306196522	其他	无	学士	计算机科学与技术	32	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	N	中国科学技术大学计算机科学与技术学院
75	王广敬	男	1995-11-12	371122199511121816	其他	无	学士	计算机软件与理论	32	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	N	中国科学技术大学计算机科学与技术学院
76	肖翔	男	1995-11-30	421302199511300013	其他	无	学士	计算机技术	32	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	N	中国科学技术大学计算机科学与技术学院
77	冯元浩	男	1994-10-14	370181199410141112	其他	无	学士	计算机应用	32	其他研究	适应智慧城市	N	中国科学技术



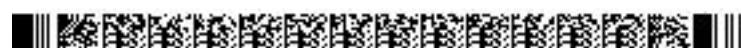
							技术		人员	市与物联网 安全目标的 安全架构和 应用示范		大学计算机科 学与技术学院	
78	陈子阳	男	1995-04-01	321324199504010012	其他	无	学士	计算机软件 与理论	32	其他研究 人员	适应智慧城 市与物联网 安全目标的 安全架构和 应用示范	N	中国科学技术 大学计算机科 学与技术学院
79	曹国栋	男	1994-10-02	370829199410024912	其他	无	学士	计算机系统 结构	32	其他研究 人员	适应智慧城 市与物联网 安全目标的 安全架构和 应用示范	N	中国科学技术 大学计算机科 学与技术学院
80	刘鹏飞	男	1994-09-28	321283199409284255	其他	无	学士	计算机技术	32	其他研究 人员	适应智慧城 市与物联网 安全目标的	N	中国科学技术 大学计算机科 学与技术学院



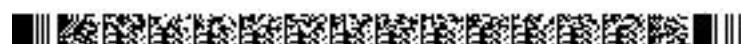
										安全架构和 应用示范				
81	汪俊军	男	1992-10-20	340828199210206314	其他	无	学士	信息管理与 信息技术	32	其他研究 人员	适应智慧城 市与物联网 安全目标的 安全架构和 应用示范	N	中国科学技 术大学计算机科 学与技术学院	
82	李安然	女	1993-08-10	342225199308100649	其他	无	学士	计算机应用 技术	32	其他研究 人员	适应智慧城 市与物联网 安全目标的 安全架构和 应用示范	N	中国科学技 术大学计算机科 学与技术学院	
83	焦锐	男	1994-10-05	210124199410051019	其他	无	学士	信息安全	32	其他研究 人员	适应智慧城 市与物联网 安全目标的 安全架构和 应用示范	N	中国科学技 术大学计算机科 学与技术学院	



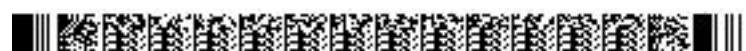
84	刘慧琦	男	1994-10-30	13042619941030031X	其他	无	学士	计算机应用技术	32	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	N	中国科学技术大学计算机科学与技术学院	
85	韩风	男	1996-02-12	37290119960212103X	其他	无	学士	信息安全	32	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	N	中国科学技术大学计算机科学与技术学院	
86	郑达人	男	1995-08-20	210303199508202013	其他	无	学士	计算机技术	32	其他研究人员	适应智慧城市与物联网安全目标的安全架构和应用示范	N	中国科学技术大学计算机科学与技术学院	
87	蒋典哲	男	1995-07-15	530324199507150019	其他	无	学士	信息安全	32	其他研究人员	适应智慧城市与物联网	N	中国科学技术大学计算机科	



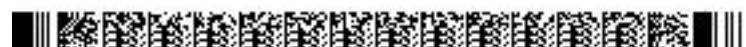
										安全目标的 安全架构和 应用示范		学与技术学院	
88	于晓静	女	1999-11-24	412824199911244721	其他	无	学士	计算机科学 与技术	32	其他研究 人员	适应智慧城市 与物联网 安全目标的 安全架构和 应用示范	N	中国科学技术 大学计算机科 学与技术学院
89	李科	男	1992-09-06	320121199209064113	其他	无	学士	信息安全	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	中国科学院信 息工程研究所 第四研究室
90	游建舟	男	1992-05-14	350822199205143914	其他	无	学士	信息安全	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和	N	中国科学院信 息工程研究所 第四研究室



										监控			
91	邹宇驰	男	1994-12-04	430121199412040411	其他	无	学士	信息安全	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	中国科学院信 息工程研究所 第四研究室
92	郑文丽	女	1991-12-23	411521199112235726	中级	无	学士	网络工程	16	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	中国科学院信 息工程研究所 第四研究室
93	郑宪东	男	1990-07-20	342423199007208574	中级	无	学士	影视动画	16	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	中国科学院信 息工程研究所 第四研究室
94	李一飞	男	1995-08-02	140225199508020038	中级	无	学士	计算机科学	24	其他研究	无安全代理	N	中国科学院信



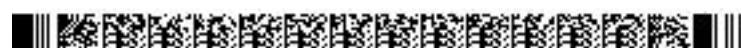
							与技术		人员	的大规模设 备智能发 现、感知和 监控		息工程研究所 第四研究室		
95	张卫东	男	1986-12-30	370612198612306034	其他	无	博士	信息安全	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	中国科学院信 息工程研究所 第四研究室	
96	李凯江	男	1990-10-21	41078119901021201X	其他	无	硕士	计算机科学 与应用	22	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	中国科学院信 息工程研究所 第四研究室	
97	贾煜璇	女	1994-10-10	130726199410100066	其他	无	硕士	信息安全	24	其他研究 人员	无安全代理 的大规模设 备智能发	N	北京交通大学 计算机与信息 技术学院	



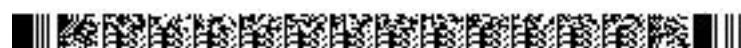
										现、感知和 监控				
98	韩冰	女	1993-02-03	130221199302030049	其他	无	硕士	信息安全	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	北京交通大学 计算机与信息 技术学院	
99	叶珩	男	1992-09-20	350502199209201518	其他	无	博士	信息安全	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	北京交通大学 计算机与信息 技术学院	
100	张骁	男	1991-05-25	410105199105250079	其他	无	博士	信息安全	22	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	北京交通大学 计算机与信息 技术学院	



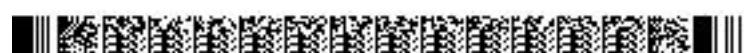
101	陈俊杰	男	1956-09-10	140102195609101250	正高级	无	博士	计算机应用技术	24	其他研究人员	无安全代理的大规模设备智能发现、感知和监控	Y	太原理工大学 计算机科学与技术学院	
102	杨玉丽	女	1979-11-23	142622197911232546	中级	无	博士	计算机应用技术	24	其他研究人员	无安全代理的大规模设备智能发现、感知和监控	Y	太原理工大学 计算机科学与技术学院	
103	于丹	女	1983-11-11	140107198311112622	其他	无	硕士	电子与通信工程	24	其他研究人员	无安全代理的大规模设备智能发现、感知和监控	N	太原理工大学 计算机科学与技术学院	
104	王潇健	女	1995-10-23	142725199510230420	其他	无	学士	计算机科学与技术	24	其他研究人员	无安全代理的大规模设	N	太原理工大学 计算机科学与	



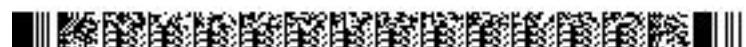
										备智能发 现、感知和 监控		技术学院	
105	张智渊	男	1996-01-07	142326199601071212	其他	无	学士	计算机技术	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	太原理工大学 计算机科学与 技术学院
106	王建华	男	1995-06-28	141125199506280210	其他	无	学士	软件工程	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	太原理工大学 计算机科学与 技术学院
107	张壮壮	男	1994-05-24	142326199405241210	其他	无	学士	计算机技术	22	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	太原理工大学 计算机科学与 技术学院



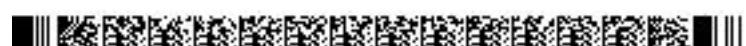
										监控			
108	刘卓华	男	1988-12-13	432522198812133751	副高级	无	博士	信息安全	24	其他研究人员	无安全代理的大规模设备智能发现、感知和监控	Y	北京富邦智慧物联科技有限公司
109	张慧超	男	1984-11-11	620103198411112338	副高级	无	硕士	信息安全	24	其他研究人员	无安全代理的大规模设备智能发现、感知和监控	Y	北京富邦智慧物联科技有限公司
110	朱蕾	男	1984-01-26	110221198401263616	副高级	无	学士	电子信息工程	24	其他研究人员	无安全代理的大规模设备智能发现、感知和监控	Y	北京富邦智慧物联科技有限公司
111	隋越	男	1990-06-23	110111199006230810	中级	无	学士	计算机科学	24	其他研究	无安全代理	Y	北京富邦智慧



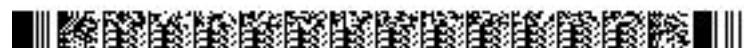
							与技术		人员	的大规模设 备智能发 现、感知和 监控		物联科技有限 公司		
112	崔佳丽	女	1990-12-04	362524199012043028	中级	无	学士	计算机科学 与技术	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	Y	北京富邦智慧 物联科技有限 公司	
113	杜海石	男	1994-05-16	210104199405163416	其他	无	学士	计算机科学 与技术	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	中国科学技术 大学计算机科 学与技术学院	
114	朱佩德	男	1990-11-03	370123199011031035	其他	无	学士	计算机科学 与技术	24	其他研究 人员	无安全代理 的大规模设 备智能发	N	中国科学技术 大学计算机科 学与技术学院	



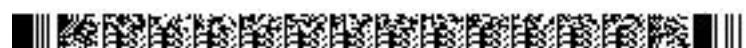
										现、感知和 监控			
115	曹书敏	女	1995-10-08	431102199510081024	其他	无	学士	计算机科学 与技术	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	中国科学技术 大学计算机科 学与技术学院
116	宓楠浣	女	1995-01-13	320202199501131527	其他	无	学士	计算机科学 与技术	24	其他研究 人员	无安全代理 的大规模设 备智能发 现、感知和 监控	N	中国科学技术 大学计算机科 学与技术学院
117	黄海平	男	1981-08-01	35042319810801001X	正高级	教授	博士	软件工程	40	其他研究 人员	基于异构标 识的安全物 联网互联互 通机制与协 议	Y	南京邮电大学 计算机学院、软 件学院、网络空 间安全学院



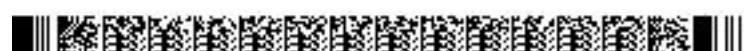
118	王少辉	男	1977-07-08	370502197707084419	副高级	副教授	学士	信息安全	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	Y	南京邮电大学 计算机学院、软件学院、网络空间安全学院	
119	沙乐天	男	1985-05-20	320302198505204413	中级	讲师	博士	信息安全	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	Y	南京邮电大学 计算机学院、软件学院、网络空间安全学院	
120	费欢	男	1990-12-20	320104199012200015	其他	无	硕士	信息网络	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	南京邮电大学 计算机学院、软件学院、网络空间安全学院	
121	陈轶	男	1987-11-11	320103198711110317	其他	无	硕士	信息网络	40	其他研究人员	基于异构标识的安全物	N	南京邮电大学 计算机学院、软	



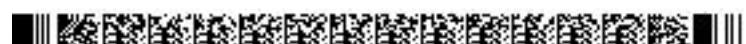
									联网互通机制与协议		件学院、网络空间安全学院	
122	刘薇	男	1991-03-21	430223199103218739	其他	无	学士	计算机应用技术	40	其他研究人员	基于异构标识的安全物 联网互通机制与协议	N 南京邮电大学 计算机学院、软件学院、网络空间安全学院
123	谢晓辉	男	1993-01-17	320682199301177954	其他	无	学士	计算机应用技术	40	其他研究人员	基于异构标识的安全物 联网互通机制与协议	N 南京邮电大学 计算机学院、软件学院、网络空间安全学院
124	郭政鑫	男	1993-07-19	340621199307190333	其他	无	学士	计算机技术	40	其他研究人员	基于异构标识的安全物 联网互通机制与协议	N 南京邮电大学 计算机学院、软件学院、网络空间安全学院



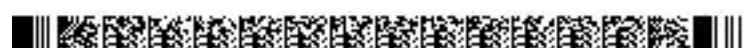
125	许平	女	1993-04-06	320611199304063121	其他	无	学士	计算机技术	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	南京邮电大学 计算机学院、软件学院、网络空间安全学院
126	刘磊	男	1990-10-10	321321199010106218	其他	无	学士	计算机技术	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	南京邮电大学 计算机学院、软件学院、网络空间安全学院
127	缪倩雯	女	1994-06-27	320602199406275321	其他	无	学士	计算机应用技术	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	南京邮电大学 计算机学院、软件学院、网络空间安全学院
128	陈静	女	1994-03-18	430528199403180048	其他	无	学士	计算机应用	40	其他研究	基于异构标	N	南京邮电大学



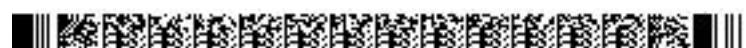
							技术		人员	识的安全物 联网互通机制与协 议		计算机学院、软 件学院、网络空 间安全学院		
129	苏川	男	1994-08-05	320981199408055711	其他	无	学士	计算机应用 技术	40	其他研究 人员	基于异构标 识的安全物 联网互通机制与协 议	N	南京邮电大学 计算机学院、软 件学院、网络空 间安全学院	
130	陈晶	女	1992-03-26	321182199203260520	其他	无	学士	软件工程	40	其他研究 人员	基于异构标 识的安全物 联网互通机制与协 议	N	南京邮电大学 计算机学院、软 件学院、网络空 间安全学院	
131	袁在平	男	1994-07-21	320821199407214934	其他	无	学士	软件工程	40	其他研究 人员	基于异构标 识的安全物 联网互通机制与协 议	N	南京邮电大学 计算机学院、软 件学院、网络空 间安全学院	



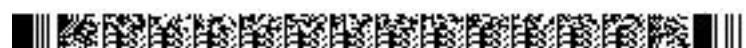
										通机制与协 议		间安全学院	
132	倪莹莹	女	1991-08-10	321321199108107489	其他	无	学士	信息网络	40	其他研究 人员	基于异构标 识的安全物 联网互联互 通机制与协 议	N	南京邮电大学 计算机学院、软 件学院、网络空 间安全学院
133	顾冰	女	1994-08-12	342426199408120222	其他	无	学士	计算机应用 技术	40	其他研究 人员	基于异构标 识的安全物 联网互联互 通机制与协 议	N	南京邮电大学 计算机学院、软 件学院、网络空 间安全学院
134	徐松	男	1995-08-01	320324199508015952	其他	无	学士	计算机应用 技术	40	其他研究 人员	基于异构标 识的安全物 联网互联互 通机制与协 议	N	南京邮电大学 计算机学院、软 件学院、网络空 间安全学院



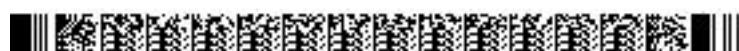
135	陈玉	女	1994-02-23	340881199402230820	其他	无	学士	计算机技术	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	南京邮电大学 计算机学院、软件学院、网络空间安全学院	
136	司娜娜	女	1993-10-05	320322199310057628	其他	无	学士	信息网络	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	南京邮电大学 计算机学院、软件学院、网络空间安全学院	
137	赵利敏	女	1993-12-21	410225199312214127	其他	无	学士	信息网络	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	南京邮电大学 计算机学院、软件学院、网络空间安全学院	
138	陈嘉琦	男	1995-01-15	320203199501152535	其他	无	学士	计算机技术	40	其他研究人员	基于异构标识的安全物	N	南京邮电大学 计算机学院、软	



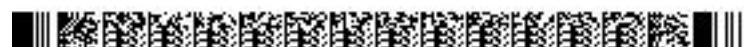
									联网互通机制与协议		件学院、网络空间安全学院	
139	陈雨昊	男	1995-03-15	321002199503157317	其他	无	学士	软件工程	40	其他研究人员	基于异构标识的安全物联网互通机制与协议	N 南京邮电大学 计算机学院、软件学院、网络空间安全学院
140	胡振超	男	1993-12-01	320105199312011618	其他	无	学士	计算机科学与技术	40	其他研究人员	基于异构标识的安全物联网互通机制与协议	N 南京邮电大学 计算机学院、软件学院、网络空间安全学院
141	李家东	男	1994-02-19	32072119940219481X	其他	无	学士	通信工程	40	其他研究人员	基于异构标识的安全物联网互通机制与协议	N 南京邮电大学 计算机学院、软件学院、网络空间安全学院



142	陈京九	男	1994-10-06	131082199410060037	其他	无	学士	计算机科学与技术	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	北京科技大学 计算机与通信工程学院
143	王辉	男	1990-07-11	370112199007110516	其他	无	学士	计算机科学与技术	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	北京科技大学 计算机与通信工程学院
144	吴霞	女	1994-11-01	429004199411013707	其他	无	学士	计算机科学与技术	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	北京科技大学 计算机与通信工程学院
145	李树仁	男	1972-10-04	342125197210043696	副高级	副教授	博士	计算机网络	24	其他研究	基于异构标	N	中国科学院计



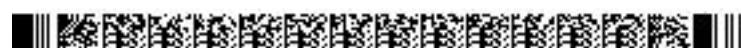
									人员	识的安全物 联网互通机制与协 议		算机网络信息 中心物联网信 息技术与应用 实验室		
146	虞路清	男	1974-12-10	362331197412103011	副高级	副教授	硕士	网络安全	24	其他研究 人员	基于异构标 识的安全物 联网互通机制与协 议	N	中国科学院计 算机网络信息 中心物联网信 息技术与应用 实验室	
147	李丹	女	1982-10-19	220202198210190924	中级	讲师	硕士	物联网	12	其他研究 人员	基于异构标 识的安全物 联网互通机制与协 议	N	中国科学院计 算机网络信息 中心物联网信 息技术与应用 实验室	
148	孙治川	男	1977-05-26	11010819770526633X	中级	讲师	学士	通信工程	10	其他研究 人员	基于异构标 识的安全物 联网互通机制与协 议	N	中国科学院计 算机网络信息 中心物联网信 息技术与应用 实验室	



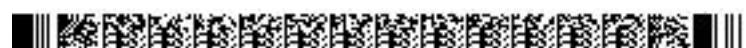
										通机制与协 议		息技术与应用 实验室		
149	唐建权	男	1995-03-14	51160219950314539X	其他	无	学士	计算机应用 技术	40	其他研究 人员	基于异构标 识的安全物 联网互联互 通机制与协 议	N	中国科学院计 算机网络信息 中心物联网信 息技术与应用 实验室	
150	李凡	男	1991-12-10	321323199112104136	其他	无	学士	软件工程	40	其他研究 人员	基于异构标 识的安全物 联网互联互 通机制与协 议	N	中国科学院计 算机网络信息 中心物联网信 息技术与应用 实验室	
151	胡松波	男	1993-04-12	420881199304122551	其他	无	学士	计算机技术	40	其他研究 人员	基于异构标 识的安全物 联网互联互 通机制与协 议	N	中国科学院计 算机网络信息 中心物联网信 息技术与应用 实验室	



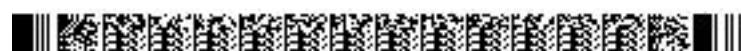
152	彭敏	男	1983-04-22	43062119830422147X	中级	讲师	博士	计算机	24	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	合肥工业大学 计算机与信息学院	
153	Alexander Keller	男	1985-02-01	C6GCX2FYY	其他	无	硕士	计算机	24	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	合肥工业大学 计算机与信息学院	
154	刘涛	男	1993-02-07	342623199302077715	其他	无	学士	计算机	24	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	合肥工业大学 计算机与信息学院	
155	张逸凡	男	1993-01-02	340103199301021010	其他	无	学士	计算机	24	其他研究人员	基于异构标识的安全物	N	合肥工业大学 计算机与信息	



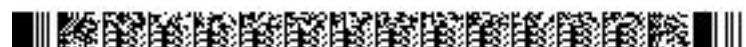
										联网互通机制与协议		学院	
156	程林松	男	1993-11-14	341282199311141835	其他	无	学士	计算机软件	40	其他研究人员	基于异构标识的安全物 联网互通机制与协议	N	清华大学软件学院
157	周青	男	1994-02-22	340823199402227011	其他	无	学士	软件工程	40	其他研究人员	基于异构标识的安全物 联网互通机制与协议	N	清华大学软件学院
158	罗优	男	1992-10-06	370982199210060019	其他	无	学士	软件工程	40	其他研究人员	基于异构标识的安全物 联网互通机制与协议	N	清华大学软件学院



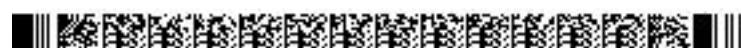
159	王朝	男	1988-05-18	210102198805185617	其他	无	学士	软件工程	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	清华大学软件学院
160	谢鹏瑾	男	1991-09-12	410122199109123444	其他	学生	学士	软件工程	40	其他研究人员	基于异构标识的安全物联网互联互通机制与协议	N	清华大学软件学院
161	刘柳燕	女	1995-10-24	432503199510242202	其他	无	学士	计算机软件与理论	40	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	中国科学技术大学计算机科学与技术学院
162	张弛	男	1995-08-18	410502199508180012	其他	无	学士	计算机应用	40	其他研究	大连接复杂	N	中国科学技术



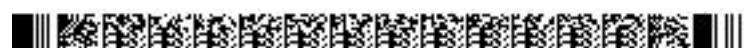
							技术		人员	异构条件下的物联网一体化安全机制		大学计算机科学与技术学院	
163	沈子喻	男	1997-03-10	220102199703103111	其他	无	学士	计算机科学与技术	40	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	中国科学技术大学计算机科学与技术学院
164	刘亮	男	1979-07-12	510223197907123912	其他	无	硕士	计算机科学与技术	40	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	西南大学电子信息工程学院
165	王曲苑	男	1994-11-17	610112199411175039	其他	无	学士	计算机科学与技术	40	其他研究人员	大连接复杂异构条件下的物联网一	N	西南大学电子信息工程学院



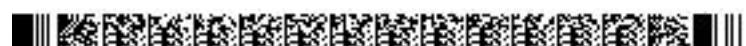
										体化安全机 制			
166	姚毅夫	男	1995-01-27	340202199501272016	其他	无	学士	计算机科学 与技术	40	其他研究 人员	大连接复杂 异构条件下的物联网一 体化安全机 制	N	西南大学电子 信息工程学院
167	焦娇	女	1994-04-14	140121199404142523	其他	无	学士	计算机科学 与技术	40	其他研究 人员	大连接复杂 异构条件下的物联网一 体化安全机 制	N	西南大学电子 信息工程学院
168	曾悦	男	1994-09-27	43052119940927661x	其他	无	学士	计算机科学 与技术	40	其他研究 人员	大连接复杂 异构条件下的物联网一 体化安全机 制	N	西南大学电子 信息工程学院



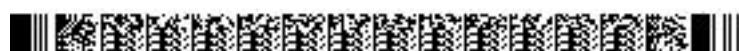
169	季鲁月	女	1994-01-11	332522199401112420	其他	无	学士	计算机科学与技术	40	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	西南大学电子信息工程学院	
170	冯浩	男	1991-08-07	140402199108073612	其他	无	硕士	计算机科学与技术	40	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	西南大学电子信息工程学院	
171	董一璠	男	1989-04-19	412301198904194037	其他	无	硕士	计算机科学与技术	20	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	西南大学电子信息工程学院	
172	夏淑芳	女	1980-08-20	211381198008202821	其他	无	硕士	计算机科学与技术	40	其他研究人员	大连接复杂异构条件下	N	西南大学电子信息工程学院	



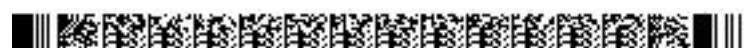
										的物联网一 体化安全机 制			
173	殷莉	女	1987-11-02	50022119871102316X	其他	无	硕士	计算机科学 与技术	40	其他研究 人员	大连接复杂 异构条件下的 物联网一 体化安全机 制	N	西南大学电子 信息工程学院
174	陈德良	男	1983-10-13	350583198310133111	中级	无	硕士	数学	24	其他研究 人员	大连接复杂 异构条件下的 物联网一 体化安全机 制	Y	北京大学前沿 交叉研究院
175	李鲁华	男	1988-03-23	371526198803236036	中级	无	硕士	计算机科学	24	其他研究 人员	大连接复杂 异构条件下的 物联网一 体化安全机 制	Y	北京大学前沿 交叉研究院



176	程超	男	1992-12-13	340104199212131011	中级	无	硕士	数学	24	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	Y	北京大学前沿交叉研究院	
177	仇文清	女	1995-04-19	310102199504191667	其他	无	学士	数据科学	40	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	北京大学前沿交叉研究院	
178	董恺	男	1985-09-18	320107198509183411	中级	无	博士	计算机网络	32	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	Y	东南大学计算机科学与工程学院	
179	肖卿俊	男	1981-12-11	360102198112115854	中级	无	博士	计算机网络	32	其他研究	大连接复杂	Y	东南大学计算	



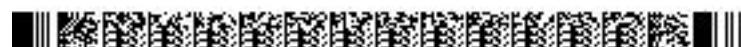
									人员	异构条件下的物联网一体化安全机制		机科学与工程学院	
180	夏翔宇	男	1994-12-15	330621199412151510	其他	无	学士	计算机应用技术	40	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	东南大学计算机科学与工程学院
181	龚志远	男	1995-07-29	32108419950729361X	其他	无	学士	计算机应用技术	40	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	东南大学计算机科学与工程学院
182	王春棉	男	1994-11-02	321321199411024010	其他	无	学士	网络空间安全	40	其他研究人员	大连接复杂异构条件下的物联网一	N	东南大学计算机科学与工程学院



										体化安全机 制				
183	郭乃瑄	男	1991-09-16	320924199109161736	其他	无	学士	计算机应用 技术	32	其他研究 人员	大连接复杂 异构条件下的物联网一 体化安全机 制	N	东南大学计算 机科学与工程 学院	
184	王永建	男	1981-02-28	410725198102281236	其他	无	硕士	计算机应用 技术	40	其他研究 人员	大连接复杂 异构条件下的物联网一 体化安全机 制	N	东南大学计算 机科学与工程 学院	
185	薛荧荧	女	1992-10-13	612701199210131860	其他	无	学士	计算机应用 技术	40	其他研究 人员	大连接复杂 异构条件下的物联网一 体化安全机 制	N	东南大学计算 机科学与工程 学院	



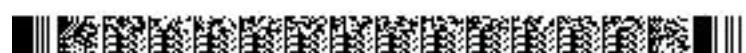
186	孟青	男	1990-01-28	371102199001280010	其他	无	硕士	计算机应用技术	40	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	东南大学计算机科学与工程学院	
187	徐威鸿	男	1995-05-25	320911199505251512	其他	无	学士	计算机应用技术	40	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	东南大学计算机科学与工程学院	
188	许丹妮	女	1993-12-17	340504199312170220	其他	无	学士	计算机应用技术	40	其他研究人员	大连接复杂异构条件下的物联网一体化安全机制	N	东南大学计算机科学与工程学院	
189	陈冷	男	1995-08-21	431122199508215834	其他	无	学士	计算机应用技术	40	其他研究人员	大连接复杂异构条件下	N	东南大学计算机科学与工程	



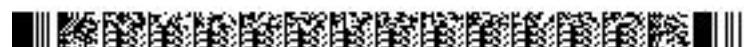
										的物联网一 体化安全机 制		学院		
190	史晓枫	男	1994-10-28	320525199410283550	其他	无	学士	计算机应用 技术	40	其他研究 人员	大连接复杂 异构条件下的 物联网一 体化安全机 制	N	东南大学计算 机科学与工程 学院	
191	徐永欢	男	1994-11-11	340221199411114953	其他	无	学士	计算机技术	40	其他研究 人员	大连接复杂 异构条件下的 物联网一 体化安全机 制	N	东南大学计算 机科学与工程 学院	
192	刘恺铮	男	1995-04-20	130825199504200059	其他	无	学士	计算机应用 技术	40	其他研究 人员	大连接复杂 异构条件下的 物联网一 体化安全机 制	N	东南大学计算 机科学与工程 学院	



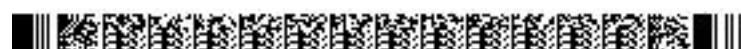
										制			
193	沈耀斌	男	1992-12-26	350212199212265017	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布式信任服务机理	N	上海交通大学电子信息与电气工程学院、计算机科学与工程系
194	张向阳	女	1990-07-22	41032319900722054X	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布式信任服务机理	N	上海交通大学电子信息与电气工程学院、计算机科学与工程系
195	万明	男	1994-12-14	34262319941214531X	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布式信任服务机理	N	上海交通大学电子信息与电气工程学院、计算机科学与工程系
196	吴哲毅	男	1997-09-27	360281199709272612	其他	无	学士	计算机科学	40	其他研究	动态跨域的	N	上海交通大学



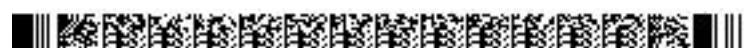
							与技术		人员	大规模分布式信任服务机理		电子信息与电气工程学院、计算机科学与工程系	
197	邹瀛	女	1982-12-17	320201198212173025	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布式信任服务机理	N	上海交通大学电子信息与电气工程学院、计算机科学与工程系
198	于跃	男	1990-02-04	340321199002040151	其他	无	学士	计算机科学与技术	36	其他研究人员	动态跨域的大规模分布式信任服务机理	N	中国科学技术大学计算机科学与技术学院
199	Sijjad Ali Khuhro	男	1991-02-07	AG4149611	其他	无	学士	计算机科学与技术	24	其他研究人员	动态跨域的大规模分布式信任服务机理	N	中国科学技术大学计算机科学与技术学院



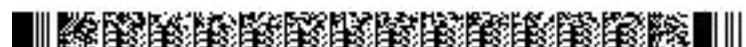
200	张帅	男	1995-04-24	341621199504243116	其他	无	学士	计算机科学与技术	36	其他研究人员	动态跨域的大规模分布式信任服务机理	N	中国科学技术大学计算机科学与技术学院	
201	白建峰	男	1995-10-20	340123199510208290	其他	无	学士	计算机科学与技术	36	其他研究人员	动态跨域的大规模分布式信任服务机理	N	中国科学技术大学计算机科学与技术学院	
202	陆长彬	男	1993-11-04	321281199311045173	其他	无	学士	计算机科学与技术	24	其他研究人员	动态跨域的大规模分布式信任服务机理	N	中国科学技术大学计算机科学与技术学院	
203	宁宇	男	1994-11-12	411123199411120014	其他	无	学士	计算机科学与技术	24	其他研究人员	动态跨域的大规模分布式信任服务机理	N	中国科学技术大学计算机科学与技术学院	
204	孟珂举	男	1994-02-24	410426199402240019	其他	无	学士	计算机科学	24	其他研究	动态跨域的	N	中国科学技术	



							与技术		人员	大规模分布式信任服务机理		大学计算机科学与技术学院	
205	孙政	男	1993-02-12	342423199302123573	其他	无	学士	计算机科学与技术	48	其他研究人员	动态跨域的大规模分布式信任服务机理	N	中国科学技术大学计算机科学与技术学院
206	解扬	男	1990-01-17	340405199001170232	其他	无	学士	计算机科学与技术	48	其他研究人员	动态跨域的大规模分布式信任服务机理	N	中国科学技术大学计算机科学与技术学院
207	WAJDY MOHAMMED SAGHEER OTHMAN	男	1985-07-04	07677348	其他	无	硕士	计算机科学与技术	36	其他研究人员	动态跨域的大规模分布式信任服务机理	N	中国科学技术大学计算机科学与技术学院
208	何乐	男	1995-05-27	440307199505274853	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布	N	清华大学计算机科学与技术



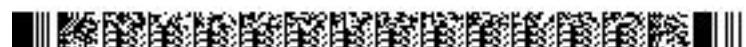
										式信任服务 机理		系	
209	朱宝玉	男	1994-01-01	12022219940101783X	其他	无	学士	计算机科学 与技术	40	其他研究 人员	动态跨域的 大规模分布 式信任服务 机理	N	清华大学计算 机科学与技术 系
210	程国华	女	1994-09-20	230123199409200600	其他	无	学士	计算机科学 与技术	40	其他研究 人员	动态跨域的 大规模分布 式信任服务 机理	N	北京理工大学 计算机学院
211	张晋鹏	男	1994-03-17	140522199403173510	其他	无	学士	计算机科学 与技术	40	其他研究 人员	动态跨域的 大规模分布 式信任服务 机理	N	北京理工大学 计算机学院
212	马宝利	男	1992-07-12	612727199207120830	其他	无	学士	计算机科学 与技术	40	其他研究 人员	动态跨域的 大规模分布 式信任服务	N	北京理工大学 计算机学院



213	陈偲祺	男	1994-12-11	110106199412116019	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布式信任服务机理	N	北京理工大学 计算机学院
214	赵梦蕉	女	1992-03-20	13073019920320182X	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布式信任服务机理	N	北京理工大学 计算机学院
215	段俊贤	女	1995-02-17	532901199502170045	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布式信任服务机理	N	北京理工大学 计算机学院
216	刘怡婷	女	1994-11-15	370684199411155221	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布式信任服务机理	N	北京理工大学 计算机学院



217	唐湘云	女	1994-11-25	431129199411253484	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布式信任服务机理	N	北京理工大学 计算机学院	
218	廖泽霖	男	1995-09-03	350481199509036518	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布式信任服务机理	N	北京理工大学 计算机学院	
219	邓雅文	女	1995-03-02	500107199503021647	其他	无	学士	计算机科学与技术	40	其他研究人员	动态跨域的大规模分布式信任服务机理	N	北京理工大学 计算机学院	
固定研究人员合计									7394	/	/	/	/	/
流动人员或临时聘用人员合计									152	/	/	/	/	/
累计									7546	/	/	/	/	/

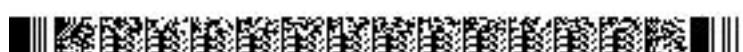


十一、经费预算

项目牵头承担单位基本情况表

表A1

填表说明: 1. 组织机构代码指企事业单位国家标准代码, 单位若已三证合一请填写单位社会信用代码, 无组织机构代码的单位填写“0000000000”; 2. 单位公章名称必须与单位名称一致; 3. 单位开户名称应与单位名称一致, 如有开户名称不一致等特殊情况, 必须提供证明文件。						
项 目 牵 头 承 担 单 位	单位名称	中国科学技术大学				
	单位性质	大专院校				
	单位主管部门	中国科学院		隶属关系	中央	
	单位组织机构代码	12100000485001086E				
	单位法定代表人姓名	包信和				
	单位开户名称	中国科学技术大学				
	开户银行(全称)	中国银行股份有限公司 合肥南城支行	汇入地点	安徽省 合肥市		
	银行账号	184203468850	银行机构代码	104361003246		
	单位所属地区	安徽省	合肥市	蜀山区		
	电子邮箱	xhba@dicp.ac.cn				
通信地址	安徽省合肥市金寨路 96 号					
邮政编码	230026					
相 关 责 任 人	项目负责人	姓名	李向阳			
		身份证号码	321025197110282833			
		工作单位	中国科学技术大学			
		电话号码	0551-63600107	手机号码	15152638982	
		电子邮箱	xiangyangli@ustc.edu.cn	邮政编码	230026	
		通信地址	安徽省合肥市金寨路96号			
	科研财务助理	姓名	刘亚男			
		电话号码	0551-63601561	手机号码	15215698839	
		传真号码	0551-63637262			
		电子邮箱	liuyanan@ustc.edu.cn	微信号	15215698839	
财务部门负责人	姓名	章晨				
	身份证号码	342521196210150055				
	电话号码	0551-63606413	手机号码	13500506053		
	电子邮箱	zhangchen@ustc.edu.cn				



项目预算表

表A2 项目编号: 2018YFB0803400

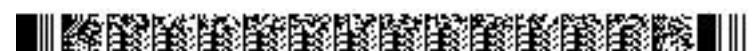
项目名称: 物联网与智慧城市安全保障关键技术研究

金额单位: 万元

课题编号	课题名称	课题承 担单位	课题 负责人	课题预算										
				经费来源					经费支出					
				中央财 政资金	其他来源资金			合计	中央财政资金			其他来 源资金	合计	
(1)	(2)	(3)	(4)		地方财 政拨款	单位 自有资金	其他资金		直接费用	间接费用	小计			
(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)				
2018YFB 0803401	适应智慧 城市与物 联网安全 目标的安 全架构和 应用示范	中国科学 技术大学	李向阳	600.00				0.00	600.00	521.60	78.40	600.00	0.00	600.00
2018YFB 0803402	无安全代 理的大规 模设备智 能发现、 感知和监 控	中国科学 院信息工 程研究所	姜建国	384.00	0.00	0.00	0.00	0.00	384.00	324.22	59.78	384.00	0.00	384.00
2018YFB 0803403	基于异构 标识的安 全物联网 互联互通 机制与协 议	南京邮电 大学	肖甫	416.00				0.00	416.00	370.38	45.62	416.00	0.00	416.00
2018YFB 0803404	大连接复 杂异构条 件下的物	东南大学	杨明	384.00				0.00	384.00	326.00	58.00	384.00	0.00	384.00



	联网一体化安全机制												
2018YFB 0803405	动态跨域的大规模分布式信任服务机理	清华大学	徐恪	396.00			0.00	396.00	342.20	53.80	396.00	0.00	396.00
累计				2180.00	0.00	0.00	0.00	2180.00	1884.40	295.60	2180.00	0.00	2180.00



十二、相关附件

国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：太原理工大学

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

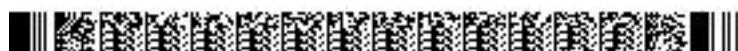
乙方为参与单位，参加人员为陈永乐。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	陈永乐	项目角色	课题骨干
子任务总经费	40.4 万元		



子任务内容	负责研究设备安全状态探测与行为智能推断方法
考核指标	支持 10 亿规模; 不少于 5 种僵尸网络物联网节点检测能力, 总体僵尸节点数量不少于 10 万。
	发表高水平论文 2 篇, 申请专利 1 项。

二、成果分配

- 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有, 不因共同承担项目(课题)而改变; 甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有, 双方共同参与研发的科技成果及相应权益归双方共同所有。
- 合作各方在合作期间因该项目研究所获取的成果, 包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划“网络空间安全”专项重点专项资助, 并标注项目编号 2018YFB0803400。

三、其他事宜

- 若本项目涉及国家秘密内容, 双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务, 不论本协议是否变更、解除或终止, 本条款长期有效。
- 本协议一式 8 份, 乙方 1 份, 甲方 7 份, 甲方其中 6 份用于项目任务书中附件使用。
- 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
- 未尽事宜, 双方本着合作共赢原则, 友好协商解决的原则另行商定。

签订协议双方签章:

甲方: 中国科学技术大学(公章) 法人代表(签章):

项目负责人: 李永东

2018年5月21日



乙方: 太原理工大学(公章)

法人代表(签章):

子任务负责人: 张永东

2018年5月18日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：南京邮电大学

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

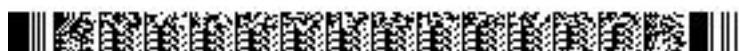
乙方为参与单位，参加人员为肖甫。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	肖甫	项目角色	课题负责人
任务总经费	197万元		
任务内容	总体负责，面向异构标识的轻量级域间及跨域身份认证和高		



	效数据隐私保护方法。
考核指标	1. 面向异构标识的轻量级域间及跨域身份认证和高效数据 隐私保护系统 1 套。 2. 发表学术论文 2 篇以上，申请专利 4 项以上。

二、成果分配

- 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
- 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划网络安全重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

- 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
- 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
- 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
- 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章）

法人代表（签章）：

项目负责人：

2018 年 5 月 11 日

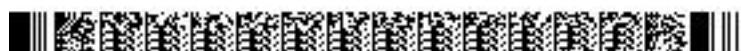


乙方：南京邮电大学（公章）

法人代表（签章）：

课题负责人：

2018 年 5 月 17 日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：合肥工业大学

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

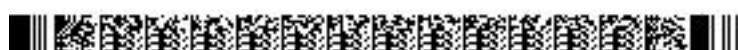
乙方为参与单位，参加人员为谷雨。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	谷雨	项目角色	研究骨干
子任务总经费	33万元		
子任务内容	负责研发基于标识的异构通信协议互联机制和安全数据路		



	由协议。
考核指标	1. 设计兼容现有物联网通信协议及路由协议的安全协议 1 种。 2. 发表论文 2 篇以上，申请专利 2 项以上。

二、成果分配

- 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
- 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划网络空间安全重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

- 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
- 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
- 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
- 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

项目负责人：



2018 年 5 月 21 日

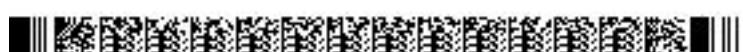


乙方：合肥工业大学（公章） 法人代表（签章）：

子任务负责人：



2018 年 5 月 18 日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：北京科技大学

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

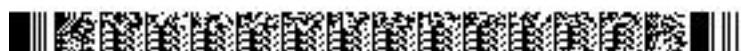
乙方为参与单位，参加人员为陈红松。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	陈红松	项目角色	研究骨干
子任务总经费	43.5万元		
子任务内容	负责完成基于标识的跨域多维分级授权和访问控制机制。		



考核指标	1. 设计物联网跨域多维分级授权及访问控制软件 1 套。 2. 发表论文 2 篇以上，申请专利 2 项以上。
------	---

二、成果分配

- 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
- 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划网络空间安全重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

- 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
- 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
- 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
- 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

项目负责人：

2018年5月21日



乙方：北京科技大学（公章）

法人代表（签章）：

子任务负责人：

2018 年 5 月 16 日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：中国科学院计算机网络信息中心

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

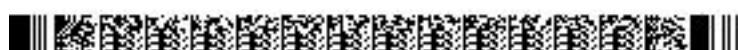
乙方为参与单位，参加人员为田野。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	田野	项目角色	研究骨干
子任务总经费	66万元		
子任务内容	负责完成异构标识的高效安全分层管理和跨域安全解析		



考核指标	1. 基于区块链、DHT 的异构标识对等解析、异构标识跨域安全解析系统 1 套。
	2. 申请专利 2 项以上，标准立项 2 项以上。

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划网络空间安全重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章）

项目负责人：李立新

法人代表（签章）：



2018 年 5 月 21 日

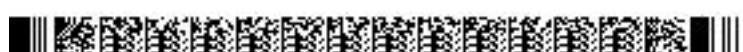
乙方：中国科学院计算机网络信息中心（公章）

子任务负责人：田飞龙

法人代表（签章）：

唐方宇

2018 年 5 月 17 日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：东南大学

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所等单位共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

乙方为参与单位，参加人员为杨明。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓 名	杨明	项目角色	课题负责人
任务总经费	139.00 万元		
任务内容	根据智慧城市的安全建设需求，针对物联网中大连接、异构数据、时延复杂等条件，研究能够与物联网节点融合的一体化安全机制，从面向异构数据的可信感知和安全存算、面向大连接、时延复杂条件的安全传输角度出发，研究设计一套		

	能与节点融合的“感传存算”一体化安全机制。
考核指标	1. 实现异构数据的可信感知技术
	2. 实现基于 PUF、物理指纹的异构节点认证方法
	3. 为智能网关、智能防火墙中隐私保护功能提供技术支持

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。

2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划物联网与智慧城市安全保障关键技术研究重点专项资助，并标注项目编号 2018YFB0803400。
月

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

项目负责人：

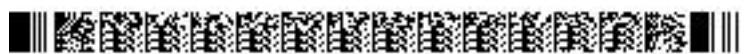
乙方：东南大学（公章） 法人代表（签章）：

任务负责人：

2018年5月21日

2018年5月17日

2



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：北京大学

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、北京大学等单位共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

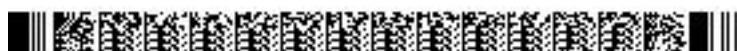
乙方为参与单位，参加人员为刘云淮。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓 名	刘云淮	项目角色	课题骨干
子任务总经费	96.00 万元		
子任务内容	根据智慧城市的安全建设需求，针对物联网中大连接、异构数据、时延复杂等条件，研究能够与物联网节点融合的一体化安全机制，重点针对面向异构数据的可信感知机制，开展安全异构数据融合等内容的研究工作。		



考核指标	1. 实现安全异构数据融合技术
------	-----------------

二、成果分配

- 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
- 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划物联网与智慧城市安全保障关键技术研究重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

- 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
- 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
- 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
- 未尽事宜，双方本着合作共嬴原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

项目负责人：

2018年5月21日

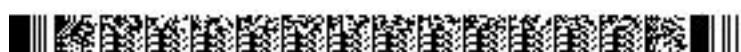


乙方：北京大学（公章）

法人代表（签章）：

子任务负责人：

2018年5月18日



国家重点研发计划项目组织实施方案

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：上海汉邦京泰数码技术有限公司

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、上海汉邦京泰数码技术有限公司等单位共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

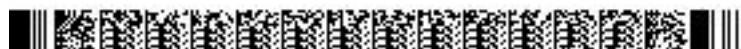
乙方为参与单位，参加人员为肖国玉。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	肖国玉	项目角色	课题骨干
子任务总经费	21.30万元		
子任务内容	根据智慧城市的安全建设需求，针对物联网中大连接、异构数据、时延复杂等条件，研究能够与物联网节点融合的一体化安全机制，重点针对面向异构数据的安全存算机制和面向大连接、时延复杂条件的安全传输机制，开展基于轻量级加		



	密的数据存算机制和基于低延迟加密的数据传输技术等内容的研究工作。
考核指标	1. 实现基于轻量级加密的数据存算机制 2. 实现基于低延迟加密的数据传输技术

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。

2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划物联网与智慧城市安全保障关键技术研究重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章）

项目负责人：



法人代表（签章）：

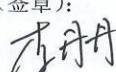


2018年5月21日

乙方：上海汉邦京泰数码技术有限公司（公章）

法人代表（签章）：

子任务负责人：



2018年5月17日

国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：北京理工大学

由中国科学技术大学牵头，清华大学、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司等单位共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

乙方为参与单位，参加人员为沈蒙。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	沈蒙	项目角色	课题骨干
子任务总经费	37.3 万元		
子任务内容	根据智慧城市的安全建设需求，针对物联网跨域服务信任的		

	问题，研究基于软件定义的强逻辑隔离安全机制以及动态跨域的大规模分布式安全信任机制与管理系统，拟从强逻辑隔离和典型应用两个方面出发，设计一套完整的管理系统。
考核指标	1. 提出 1 个典型应用，并在第三方平台上得到验证 2. 为体系结构和平台提供应用支持

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划网络空间安全重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 9 份，乙方 2 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共贏原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

项目负责人：



2018 年 5 月 21 日

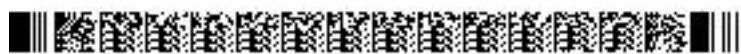
乙方：北京理工大学（公章）

法人代表（签章）：

子任务负责人：



2018 年 5 月 17 日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：中兴通讯股份有限公司（公司）

由中国科学技术大学牵头，清华大学、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司等单位共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

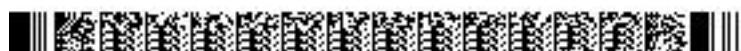
乙方为参与单位，参加人员为甘玉玺。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	甘玉玺	项目角色	课题骨干
子任务总经费	37.3 万元		
子任务内容	根据智慧城市的安全建设需求，针对物联网跨域服务信任的		



	问题，设计并实现动态跨域的大规模分布式安全信任机制与管理系统，拟从理论基础和典型应用三个方面出发，设计一套完整的管理系统。
考核指标	1. 提出 1 个典型应用，并在第三方平台上得到验证 2. 为体系结构和平台提供应用支持

二、成果分配

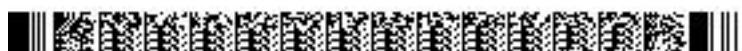
1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划网络空间安全重点专项资助，并标注项目编号 2018YFB0803400。

三、合规

1. 履行合同时，开发方需遵守所有美国出口管制法律的规定。若无有效的许可豁免或许可例外，而法律又有其他要求的，则开发方应按照要求负责在出口硬件、技术及软件，或者提供技术支持时申请许可，或者获得其他方式的审批。
2. 若有非美国主体将参与合同履行，且在参与过程中会接触到出口管制所管控的技术数据或软件时，若有需要，在其参与之前开发方需申请出口许可证。
3. 开发方需满足所有法律项下，适用许可或许可例外时的文档保存要求。
4. 开发方需确保其分包商也符合本合同中出口管制合规要求。

四、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。
甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。



(此页为盖章签字页)

签订协议双方签章:

甲方: 中国科学技术大学(公章)

项目负责人:



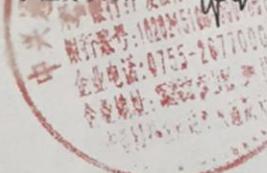
法人代表(签章):



2018年7月31日

乙方: 中兴通讯股份有限公司(公章)

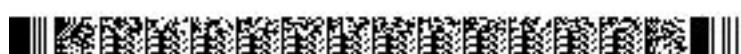
子任务负责人:



法人代表(签章):



2018年7月20日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：国家信息中心

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

乙方为参与单位，参加人员为张延强。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	张延强	项目角色	研究骨干
子任务总经费	130 万元		

子任务内容	参与一体化安全关键技术，构建适应智慧城市与物联网安全目标的模型和体系框架
考核指标	<ol style="list-style-type: none"> 1. 提出 1 项智慧城市一体化安全关键技术 2. 提出 1 个适应智慧城市与物联网安全目标的模型 3. 提出 1 个适应智慧城市与物联网安全目标的体系框架

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划“物联网与智慧城市安全保障关键技术研究”重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 10 份，乙方 3 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

项目负责人：

乙方：国家信息中心（公章） 法人代表（签章）：

子任务负责人：

2018年5月21日

2018年5月17日

国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：北京泰豪智能工程有限公司

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学等单位共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

乙方为参与单位，参加人员为马益荣。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	马益荣	项目角色	研究骨干
子任务总经费	65 万元		
子任务内容	根据智慧城市的安全建设需求，针对智慧城市通用的体系架构，研究智慧城市安全保障技术架构，拟从安全技术体系、		

	管理体系、运维体系三个角度出发，设计一套完整的安全保障体系。
考核指标	1. 提出 6 个典型应用，并在第三方平台上得到验证 2. 为体系结构和平台提供应用支持

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。

2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划“物联网与智慧城市安全保障关键技术研究”重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。

2. 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。

3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。

4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

项目负责人：

乙方：北京泰豪智能工程有限公司（公章） 法人代表（签章）：

子任务负责人：

2018年5月21日

2018年5月18日

国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：北京交通大学

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

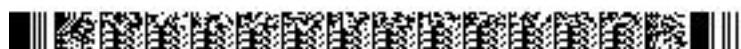
乙方为参与单位，参加人员为李强。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	李强	项目角色	课题骨干
子任务总经费	40.4 万元		



子任务内容	负责研究多维属性融合的设备识别模型及方法
考核指标	<p>1. 识别设备的种类≥ 10种，数量支持10亿规模；识别准确率不低于95%。</p> <p>2. 发表高水平论文2篇，申请专利1项。</p>

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。

2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划“网络空间安全”专项重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。

甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。

2. 本协议一式8份，乙方1份，甲方7份，甲方其中6份用于项目任务书中附件使用。

3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。

4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

项目负责人：

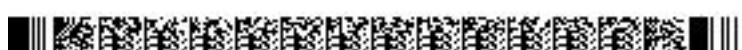
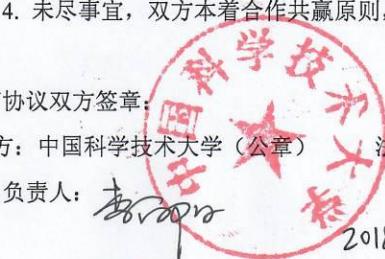
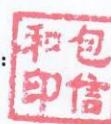
乙方：北京交通大学（公章） 法人代表（签章）：

子任务负责人：

2018年5月21日

2018年5月17日 宁波

2



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：中移物联网有限公司

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网有限公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

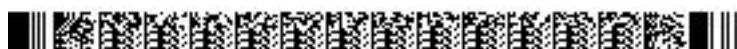
乙方为参与单位，参加人员为肖青。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓 名	肖青	项目角色	研究骨干
子任务总经费	65 万元		



子任务内容	研制安全物联网原型平台。
考核指标	1. 构建 1 套用于支持一体化安全关键技术的原型平台 2. 为体系结构和平台提供应用支持

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划“物联网与智慧城市安全保障关键技术研究”重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

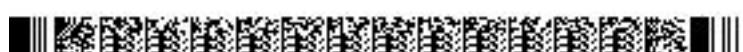
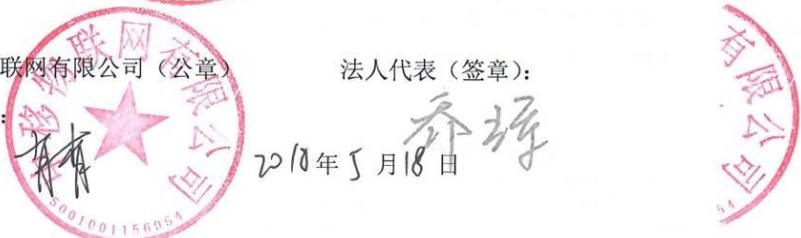
项目负责人：



乙方：中移物联网有限公司（公章）

法人代表（签章）：

子任务负责人：



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：上海交通大学

由中国科学技术大学牵头，清华大学、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司等单位共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

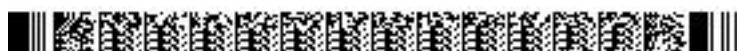
乙方为参与单位，参加人员为王磊。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓 名	王磊	项目角色	课题骨干
子任务总经费	60.6 万元		
子任务内容	根据智慧城市的安全建设需求，针对物联网跨域服务信任的		



	问题，研究于分布式共识的跨域身份信息与认证技术，拟从物联网节点操作系统可信增强、可信度量和身份信息认证三个方面出发，研究物联网跨域的协作机制。
考核指标	1. 在第三方平台上得到验证 2. 为体系结构和平台提供应用支持

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划网络空间安全重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章）

项目负责人：

李保阳

法人代表（签章）：

和包印信

2018年5月17日

乙方：上海交通大学（公章）

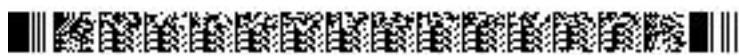
子任务负责人：

王磊

法人代表（签章）：

林忠钦

2018年5月21日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：北京奇安信科技有限公司

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

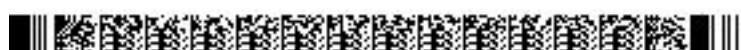
乙方为参与单位，参加人员为李强。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	李强	项目角色	研究骨干
子任务总经费	22 万元		



子任务内容	研究网络安全平台，提供防火墙，入侵防御，网站防篡改，安全审计等服务。
考核指标	1. 构建 1 套具有防火墙、入侵防御等服务的网络安全平台

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划“物联网与智慧城市安全保障关键技术研究”重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

项目负责人：

乙方：（公章）北京奇安信科技有限公司

法人代表（签章）：

子任务负责人：

2018年 5月 18 日

2018年 5月 21 日

国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：清华大学

由中国科学技术大学牵头，清华大学、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司等单位共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

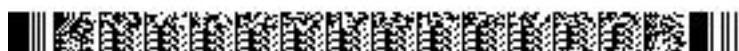
乙方为参与单位，参加人员为徐恪。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓 名	徐恪	项目角色	课题负责人
任务总经费	223.6 万元		
任务内容	根据智慧城市的安全建设需求，针对物联网跨域服务信任的问题，研究基于软件定义的强逻辑隔离安全机制、基于身份		



	和角色的授权策略映射以及动态跨域的大规模分布式安全信任机制与管理系统，拟从强逻辑隔离、授权管控和典型应用三个方面出发，设计一套完整的管理系统。
考核指标	1. 提出 1 个典型应用，并在第三方平台上得到验证 2. 为体系结构和平台提供应用支持

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划网络空间安全重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章）

法人代表（签章）：

项目负责人：

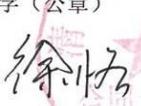


2018 年 5 月 21 日

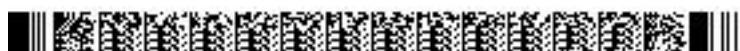
乙方：清华大学（公章）

法人代表（签章）：

课题负责人：



2018 年 5 月 18 日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：中国科学院信息工程研究所

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

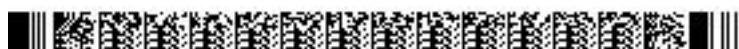
乙方为参与单位，参加人员为姜建国。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	姜建国	项目角色	课题负责人
任务总经费	222.4万元		



任务内容	负责研究无打扰、跨网跨域、主被动结合的设备发现，负责物联网安全监管子平台的研发。
考核指标	支持 10 亿规模设备发现。
	发表论文 3 篇，申请专利 3 项。

二、成果分配

- 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
- 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划“网络空间安全”专项重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

- 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
- 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
- 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
- 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章）

项目负责人：

法人代表（签章）：



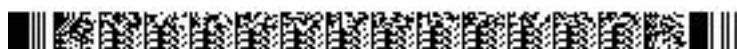
2018年 5月 18 日

乙方：中国科学院信息工程研究所（公章）

课题负责人：

法人代表（签章）：

2018年 5月 24 日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：北京富邦智慧物联科技有限公司

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

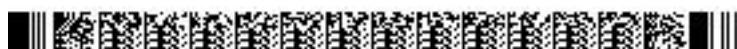
乙方为参与单位，参加人员为刘伟。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓 名	刘伟	项目角色	课题骨干
子任务总经费	40.4 万元		



子任务内容	在消防领域验证课题二的技术，配合项目开展智慧社区应用示范建设
考核指标	在具备 10 亿设备规模的应用场景中验证课题二关键技术 申请专利 3 项。

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划“网络空间安全”专项重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

项目负责人： 李海川

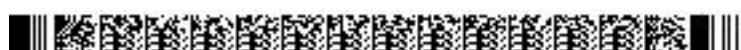
2018年5月21日



乙方：北京富邦智慧物联科技有限公司（公章） 法人代表（签章）：

子任务负责人：

2018年5月18日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：西南大学

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、西南大学等单位共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

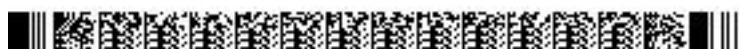
乙方为参与单位，参加人员为杨元元。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓 名	杨元元	项目角色	课题骨干
子任务总经费	85.10 万元		
子任务内容	根据智慧城市的安全建设需求，针对物联网中大连接、异构数据、时延复杂等条件，研究能够与物联网节点融合的一体化安全机制，重点针对面向异构数据的安全存算机制和面向物联网节点的安全和性能优化机制，开展基于功能加密的数		



	据存算机制和面向节点资源受限的传算结合机制等内容的研究工作。
考核指标	1. 实现基于功能加密的数据存算机制 2. 实现面向节点资源受限的传算结合机制

二、成果分配

1. 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。

2. 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划物联网与智慧城市安全保障关键技术研究重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

1. 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
2. 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
3. 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
4. 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章）

项目负责人：李云波

法人代表（签章）：



2018年5月14日

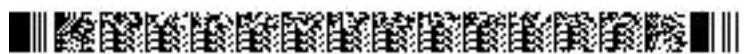
乙方：西南大学（公章）

项目负责人：杨红

法人代表（签章）：



2018年5月18日



国家重点研发计划项目组织实施协议

甲方（承担单位）：中国科学技术大学

乙方（参与单位）：清华大学

由中国科学技术大学牵头，清华大学、东南大学、南京邮电大学、中国科学院信息工程研究所、中移物联网公司、北京泰豪智能工程有限公司、北京奇安信科技有限公司、国家信息中心、北京富邦智慧物联科技有限公司、北京交通大学、太原理工大学、中国科学院计算机网络信息中心、合肥工业大学、北京科技大学、北京大学、西南大学、上海汉邦京泰数码技术有限公司、上海交通大学、北京理工大学、中兴通讯股份有限公司共同申请的国家重点研发计划项目“物联网与智慧城市安全保障关键技术研究”（项目编号：2018YFB0803400）于2018年7月开始实施。为保证项目的顺利实施，根据国家相关法律和管理办法，结合甲乙双方的科研优势，在原有合作的基础上，双方决定依照真诚合作、平等互利的原则达成如下组织实施协议：

一、合作内容

1. 甲方为项目牵头单位，项目负责人为李向阳；

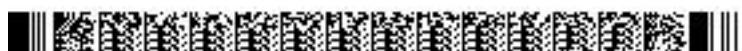
乙方为参与单位，参加人员为曹志超。

在该项目的实施过程中，各单位均承诺提供充分的人力、物力参与本项目子任务实施工作；在项目执行过程中，精心组织、密切协作，按任务书要求完成子任务目标；执行国家专项管理办法和经费管理办法，按照任务相关性、政策相符性和经济合理性原则使用经费。

2. 甲方将按照现行的国家重点研发计划项目管理办法和经费管理办法对乙方承担的子任务进行监督和管理，可向乙方获取项目研究相关的技术资料用于本项目的研究。

3. 乙方研究团队责任分工、考核指标、经费分配情况如下表所示：

姓名	曹志超	项目角色	研究骨干
子任务总经费	76.5万元		
子任务内容	负责研究基于多元特征的多类型可靠标识生成方法。		



考核指标	1. 物联网设备标识生成系统 1 套。 2. 发表学术论文 2 篇以上，申请专利 2 项以上。
------	--

二、成果分配

- 甲乙双方在项目执行之前各自所获得的知识产权及相应权益均归各自所有，不因共同承担项目（课题）而改变；甲乙双方在项目研究过程中独立研究产生的科技成果归研发方所有，双方共同参与研发的科技成果及相应权益归双方共同所有。
- 合作各方在合作期间因该项目研究所获取的成果，包括论文、专著、专利以及鉴定、成果报道等均须注明国家重点研发计划网络空间安全重点专项资助，并标注项目编号 2018YFB0803400。

三、其他事宜

- 若本项目涉及国家秘密内容，双方应按国家保密管理规定做好保密工作。甲乙双方均对对方提供的技术情报和资料承担保密义务，不论本协议是否变更、解除或终止，本条款长期有效。
- 本协议一式 8 份，乙方 1 份，甲方 7 份，甲方其中 6 份用于项目任务书中附件使用。
- 合作双方均按要求遵守国家重点研发计划项目规定的诚信承诺。
- 未尽事宜，双方本着合作共赢原则，友好协商解决的原则另行商定。

签订协议双方签章：

甲方：中国科学技术大学（公章） 法人代表（签章）：

项目负责人：



2018 年 5 月 21 日

乙方：清华大学（公章）

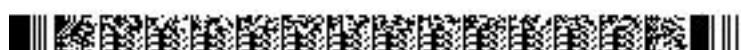
法人代表（签章）：

子任务负责人：

曹志超



2018 年 5 月 18 日



任务书签署

甲乙双方根据《国务院关于改进加强中央财政科研项目和资金管理的若干意见》(国发[2014]11号)、《国务院印发关于深化中央财政科技计划(专项、基金)管理改革方案的通知》(国发[2014]64号)、《科技部 财政部关于印发<国家重点研发计划管理暂行办法>的通知》(国科发资[2017]152号)、《财政部 科技部关于印发<国家重点研发计划资金管理办法>的通知》(财科教[2016]113号)、《科技部财政部关于印发<中央财政科技计划(专项、基金等)监督工作暂行规定>的通知》(国科发政[2015]471号)等有关规定,以及有关法律、政策和管理要求,依据项目立项通知,签署本任务书。

专业机构(甲方):

法定代表人签字(签章):

(公章)

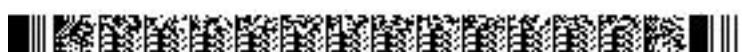
年 月 日

项目牵头承担单位(乙方):

法定代表人签字(签章):

(公章)

年 月 日



项目负责人签字（签章）：

年 月 日

推荐单位（盖章）

年 月 日

