

2025 年度拟提名陕西省科技进步奖项目公示内容

一、项目名称

芯片设计安全评估技术

二、提名者及提名意见

提名者：

陕西省教育厅

提名意见：

该项目围绕国家网络空间安全和集成电路重点发展战略，聚焦芯片安全热点前沿领域，面向自主芯片设计安全检测需求，针对芯片安全评估中存在的“安全难建模”、“属性难验证”、“漏洞难检测”等关键挑战，在芯片设计安全性评估领域开展了体系化的创新研究，形成了芯片设计安全行为分析与建模技术、芯片设计安全脆弱性特征提取与智能匹配技术和芯片设计安全属性验证与脆弱性搜索挖掘技术等代表性的创新成果，构建了智能化、形式化、自动化、标准化的芯片设计安全评估技术，在已知安全脆弱性特征精准匹配和未知安全脆弱性搜索挖掘方面取得突出效果，技术水平国内领先、国际先进。项目结合创新研究成果，开展了芯片设计安全评估与脆弱性检测方面的自主工具研发，并在中国科学院信息工程研究所、航天恒星科技有限公司、西安微电子技术研究所、龙芯中科和成都环宇芯科技有限公司等单位研发的多款国产芯片设计安全检测中实际应用，检测到某国产处理器、航天专用片上系统和星载专用芯片设计中的安全风险，为多个型号任务的研发提供了有力技术保障，取得经济效益超 1.7 亿元。成果为增强自主芯片设计安全性提供了有效的理论、技术和工具支撑，有助于从芯片底层筑牢网络安全的硬件根基，抵御芯片安全攻击所造成的严重影响和经济损失，具有良好的社会和经济效益。成果材料属实、齐全、规范，人员排序无争议，符合陕西省科学技术进步奖提名条件。

提名该项目为陕西省科学技术进步奖二等奖。

三、项目简介

网络空间安全和集成电路是国家重点发展战略。芯片安全属于两大战略的交叉领域，是备受关注的热点前沿方向。芯片作为计算系统的硬件核心和网络空间的物理根基，其安全性对网络空间上层建筑的安全性至关重要，是网络安全最后一道关闸。然而，网络攻击的战火已经蔓延至硬件层面，芯片已成为新的攻击热点，导致武器装备、民用基础设施和个人计算设备中芯片安全问题频发，对网络空间安全造成了严重威胁。芯片是我国面临的关键技术难题，国家正大力推进核心芯片的自主替代，然而，自主可控不等于安全可靠，即使是完全自主设计的芯片也可能存在安全脆弱性。该项目研究并构建体系化芯片设计安全评估技术，有助于提升自主芯片的安全可信程度，筑牢网络安全的硬件基础，为网络安全提供可靠的硬件根基，服务于国家网络空间安全和集成电路发展战略。

现有芯片设计流程普遍关注面积、延迟和功耗等性能指标，所采用的功能性电路模型缺少安全相关的属性和参数，难以实现安全性建模与评估。项目针对芯片安全评估中存在的“安全难建模”、“属性难验证”、“漏洞难检测”等关键挑战，系统地开展了芯片设计安全脆弱性评估技术研究，形成了智能化、形式化、自动化、标准化的体系化芯片设计安全评估技术，有助于在设计阶段以较低代价检测并消除芯片中潜在的安全隐患，避免安全脆弱芯片需重新设计和流片加工导致的高额成本，以及利用芯片安全脆弱性发起攻击所导致的严重后果和经济损失，具有良好的社会和经济效益。项目的代表性创新如下：

1.芯片设计安全行为分析与建模技术。在国际上开创性地提出了细粒度信息流安全建模技术，构建了附加安全维度的芯片设计安全模型，建模精度提升达 28.8%，为芯片设计安全评估提供了数学基础，研究工作处于国际领跑地位。

针对现有功能性电路设计模型缺乏安全维度，难以实现安全性分析与建模的根本不足，提出了芯片设计细粒度信息流分析技术，从信息传播的角度实现对信息泄露、信息篡改、非授权访问、侧信道、恶意逻辑等安全相关行为的分析，实现了芯片设计中全部逻辑信息流的精确度量，度量精度达到二进制位；提出了一种芯片设计细粒度安全建模技术，为功能性芯片设计模型附加安全属性维度，克服了现有芯片设计模型只能实现功能正确性和性能评估，难以实现安全属性建模和验证的根本不足，为芯片设计安全性分析提供了数学模型。

2.芯片设计安全脆弱性特征提取与智能匹配技术。创新性地提出了一种融合结构和行为特征的安全脆弱性特征自动提取和基于深度学习模型的脆弱性特征匹配技术，已知特征脆弱性检测率达到 98.5%以上，为当前国际最佳水平。

针对芯片安全脆弱性类型复杂多变，脆弱性特征缺乏统一范式，脆弱性特征数据分散不显著、分布不均匀导致的脆弱性特征提取困难问题，提出了融合芯片设计结构和行为特征的安全脆弱性特征提取技术，在显著提升特征提取自动化程度的同时，提升了所提取特征的准确性。提出了基于智能化特征匹配的安全脆弱性检测技术，实现了已知特征安全脆弱性的精准检测，克服了传统方

法耗时久效率低、误报和漏报率高等弊端，并具有很好的可解释性，研究水平达到国际领先，为精准分析芯片脆弱性提供了有力支撑。

3.芯片设计安全属性验证与脆弱性搜索挖掘技术。在国际上开创性地提出属性驱动的硬件安全技术，实现了属性相关的状态空间搜索和属性驱动的脆弱性挖掘，在未知安全脆弱性发掘能力上取得显著优势，研究水平处于国际前沿。

针对芯片设计安全漏洞隐蔽性高，难以实现有效检测，以及芯片设计流片加工后安全漏洞难以消除的痛点问题，提出了一种芯片安全属性形式化验证方法，实现了芯片设计关键安全属性的形式化证明，显著提升了芯片设计安全评估方法的数学严谨性和分析完备性。提出了一种基于属性验证的安全脆弱性搜索挖掘技术，形成了属性驱动的状态空间搜索和安全脆弱性检测方法，解决了高隐蔽性芯片设计安全脆弱性检测难题，研究工作处于国际前沿。所提出的技术有效融合了标准电子设计自动化语言和工具，有效提升了芯片设计安全评估的自动化程度。

结合上述创新研究，获发明专利授权 18 项、软件著作权 12 项，在知名期刊和会议上发表论文 100 余篇，出版专著 1 部（科学出版社），**取得国内首个自主挖掘的 RISC-V 处理器设计上可远程利用的中危漏洞**，受到 CNCERT 国家工程研究中心和人民网等媒体专题报道。

项目多项任务来源课题分别经科技部、国家自然科学基金委、陕西省科技厅、中国科学院信息工程研究所、北京计算机技术及应用研究所等机构组织专家评审并通过验收。项目研究的芯片设计安全评估技术以及所研发的芯片设计安全脆弱性分析软件已通过安徽安正测评技术有限公司 CMA 认证，所研发的纳米级芯片硬件综合安全评估关键技术研究项目处理器集成电路设计脆弱性检测与形式化验证工具已通过航天中认软件测评科技(北京)有限责任公司 CNAS 认证。

项目研究成果已经在中国科学院信息工程研究所、航天恒星科技有限公司、西安微电子技术研究所、龙芯中科、成都环宇芯科技有限公司等 10 余家单位的关键芯片设计安全检测中实际应用，**检测到某国产处理器设计中存在的信息流安全风险路径、通用星载导航单机中广泛应用的 SoC 电路设计在辐照极端环境下存在的意外解锁的设计安全隐患和型号用以太网接口芯片设计中某校验模块存在的设计缺陷问题**，有效提升了自主芯片设计的安全性，取得经济效益超 1.7 亿元。

该项目开展了芯片设计安全评估技术体系化研究及应用验证，并在此基础上构建了自主芯片设计安全检测工具和检测能力，能够为保障自主芯片设计安全性提供有效的理论、技术和工具支撑，从芯片底层构筑网络安全防线，具有良好的社会经济效益。

四、客观评价

该项目任务来源课题均已顺利通过验收，支撑了工具研发和应用验证；所研发的芯片设计安全验证与漏洞检测软件已通过权威机构检测；项目成果已应用于多款自主设计芯片的安全评估，产生了良好的社会效益，理论成果受到包括多位 IEEE Fellow 在内的知名硬件安全专家的积极评价。

(1) 项目验收结论

1) 2025 年 1 月 17 日，国家重点研发计划课题绩效评价专家组，对西北工业大学胡伟承担的国家重点研发计划“网络空间安全治理”重点专项课题：处理器集成电路设计脆弱性检测与形式化验证（课题编号：2021YFB3100901）进行了课题绩效评价材料审查。评审组一致认为该项目达到了任务书要求的考核指标，材料完整规范，符合绩效评价要求。

2) 2025 年 3 月 27 日，国家自然科学基金委有关专家，对西北工业大学胡伟承担的国家自然科学基金面上项目：基于联合信息流分析的细粒度标准化硬件安全模型与度量研究（项目批准号：62074131）进行了验收。评审组一致认为该项目完成了合同规定的任务，准予结题。

3) 2021 年 3 月 29 日，国家自然科学基金委有关专家，对西北工业大学慕德俊承担的国家自然科学基金面上项目：基于门级信息流分析的集成电路设计安全漏洞检测技术研究（项目批准号：61672433）进行了验收。评审组一致认为该项目完成了合同规定的任务，准予结题。

4) 2017 年 3 月 23 日，国家自然科学基金委有关专家，对西北工业大学胡伟承担的国家自然科学基金青年项目：基于细粒度信息流分析的高可靠系统安全验证方法研究（项目批准号：61303224）进行了验收。评审组一致认为该项目完成了合同规定的任务，准予结题。

5) 2024 年 3 月 26 日，国家自然科学基金委有关专家，对西北工业大学毛保磊承担的国家自然科学基金青年项目：基于信息流模型的硬件时间侧信道检测与量化评估（项目批准号：62004176）进行了验收。评审组一致认为该项目完成了合同规定的任务，准予结题。

(2) 权威机构检测报告

1) 安徽安正测评技术有限公司 2020 年 10 月 19 日至 2020 年 11 月 4 日对“基于门级细粒度信息流分析的硬件安全验证与漏洞检测软件”进行了测试，测试结果如下：该软件属于通用应用软件，实现了基于门级细粒度信息流分析的硬件安全验证与漏洞检测功能，具体包括门级细粒度信息流模型生成、门级细粒度信息流分析、信息流泄露路径搜索等功能。

2) 航天中认软件测评科技（北京）有限责任公司 2024 年 11 月“纳米级芯片硬件综合安全评估关键技术研究项目处理器集成电路设计脆弱性检测与形式化验证”进行了验收测试，并获得专家组一致通过。

(3) 应用成效评价

该项目研究成果已在中国科学院信息工程研究所、航天恒星科技有限公司、

西安微电子技术研究所等单位的一线产品或科研课题中成功应用。应用结果表明：该项目研发的芯片设计安全脆弱性分析技术提高了硬件系统的安全性和可靠性，解决了传统安全防护技术无法满足硬件安全的关键问题，提升了国产硬件系统安全性与可靠性，产生经济效益超 1.7 亿元。

(4) 同行学术评价

1) IEEE Fellow Mark Tehranipoor 教授等指出项目团队提出的 GLIFT 技术是一种**显示化污点和逻辑值传播的强有力技术 (powerful technique)**。

2) IEEE Fellow Norman Chang 等指出项目团队提出的 GLIFT 方法能够**更准确 (more accurate)**地实现路径敏化分析。

3) 知名硬件安全专家 Hassan Salmani 将项目团队提出的 GLIFT 方法作为一种**精确度量和控制 (precisely measure and manage)**底层硬件中数据流的方法。

4) 知名硬件安全专家 Domenic Forte 教授和 IEEE Fellow Mark Tehranipoor 教授等认为**检查敏感数据完整性非常重要 (important to check the integrity of the sensitive data)**，并将项目团队提出的门级信息流分析方法 (gate-level information flow tracking) 作为最近的**代表性方法**。

5) Cycuity 公司联合创始人兼首席技术官 Jason Oberg 博士指出该公司的 Radix 商用安全验证工具参考了完成人所提出的信息流分析技术，并评价道**该技术为硬件设计机密性、完整性、可用性等安全目标提供了强有力的保障 (strong guarantees)**。

6) 知名硬件安全专家 Rainer Leupers 教授等指出项目团队的工作是一种**验证机密性和完整性属性 (prove security properties such as confidentiality and integrity)**的可靠方法 (a solid methodology)。

7) 知名硬件安全专家 Daniel Große 和 Rolf Drechsler 等指出 IFT 技术 (IFT techniques) 是一种**保障安全策略的有效途径 (effective in enforcing security policies)**，并将项目团队提出的 GLIFT 技术作为硬件层 IFT 技术的**代表性工作**。

8) 知名硬件安全专家 Kaveh Razavi 教授等发表在安全领域顶会 USENIX 上的论文指出项目团队的工作是一种在特定场景下动态证明机密性、完整性、隔离性、时间一致性、设计完整性属性的**典型方法 (canonical properties covered by dynamic IFT)**，能够**避免静态方法面临的状态爆炸问题 (immune to the state explosion problem)**。

五、应用情况

该项目研究成果已成功应用于我国多家企业，在技术功能增益验证和推动企业经济效益增长方面均取得良好成效。应用企业涉及面广泛，包括中国科学院信息工程研究所、航天恒星科技有限公司、西安微电子技术研究所等国内重点行业、重点单位，详见下表。应用结果表明：该项目研发的芯片设计安全评估技术提高了硬件系统的安全性和可靠性，解决了传统安全防护技术无法满足硬件安全关键问题，提高了国产硬件系统安全性与可靠性，并产生显著的经济和社会效益。

主要应用单位情况表

序号	单位名称	应用的技术	应用对象及规模	应用起止时间	单位联系人
1	西安微电子技术研究所	芯片设计安全评估技术	以太网接口等产品的基础产品应用验证	2020.12-2022.03	田家源
2	航天恒星科技有限公司	芯片设计安全脆弱性分析技术及应用	SoC 芯片设计安全验证	2022.03-2022.12	穆峻
3	中国科学院信息工程研究所	基于细粒度信息流分析的芯片设计安全验证与漏洞检测技术	CPU 核安全性测试任务	2020.04-2020.09	朱子元
4	山东航天电子技术研究所	电路设计安全评估技术	多款航天器用产品设计阶段安全性评估	2020.12-2022.02	倪卫星
5	西安启明星辰信息技术有限公司	芯片设计脆弱性特征自动提取与智能匹配技术	外购 IP 模块安全检测	2021.02-2023.03	张文晓
6	北京控制与电子技术研究所	FPGA 设计信息流安全建模与形式化验证技术	型号产品 FPGA 代码设计安全性检测	2023.04-2024.04	王峰
7	深圳市纽创信安科技开发有限公司	密码芯片设计安全验证与脆弱性检测技术	密码 IP 核和密码芯片设计安全性检测	2020.10-2024.01	梁凯
8	成都环宇芯科技有限公司	密码 IP 核设计安全形式化验证与信息泄漏检测技术	HYS2210 型 RISC-V 处理器芯片内置密码模块安全性测评业务	2023.06-2025.03	闫要岗
9	龙芯中科技术股份有限公司	纳米级芯片硬件综合安全评估关键技术研究	某型国产处理器芯片设计安全性测评业务	2023.04-2024.11	吴江
10	北京轩宇空间科技有限公司	芯片设计安全评估技术	型号用核心芯片设计流片前安全评估	2020.12-2022.03	李宾

(1) 西安微电子技术研究所：芯片设计安全评估技术已在我单位以太网接口等产品的基础产品应用验证工作中实际应用，帮助设计人员检测到了某校验模块

存在的设计缺陷问题，避免了芯片重新流片的经济损失和潜在的安全风险，为型号用核心芯片设计流片前安全评估提供了新技术途径和有力支撑。

(2) 航天恒星科技有限公司：联合研发了芯片设计安全脆弱性分析技术。基于此形成的芯片设计阶段安全脆弱性测评工具，具有逻辑建模、基于信息流的自动形式化走查，逻辑脆弱点定位及逻辑安全加固等功能。测评工具应用于两款 SoC 芯片的研制过程，成功在设计阶段检查出极端边界条件下的设计缺陷两项。

(3) 中国科学院信息工程研究所：基于细粒度信息流分析的芯片设计安全验证与漏洞检测技术在我单位实施的 CPU 核安全性测试任务中，为其安全性测试提供了技术支撑，检测到设计中存在的信息流安全风险，通过对比人工检测结果分析，该检测工具可帮助设计人员在硬件设计阶段提升设计的安全性。

(4) 山东航天电子技术研究所：电路设计安全评估技术已在我单位多款航天器用产品设计阶段安全性评估中实际应用，成功在设计中排查容错设计缺陷等安全使用风险，技术水平先进，有助于提升我单位航天器用核心电路设计的安全性和可靠性，为型号研发任务提供了有效技术保障。

(5) 西安启明星辰信息技术有限公司：芯片设计脆弱性特征自动提取与智能匹配技术已在我公司芯片设计外购 IP 模块安全检测中实际应用，典型芯片脆弱性检测和定位精度达到 98% 以上，较其它方法提升 13% 以上，相关技术有实质性创新，技术水平达到国际前沿，产生了重大经济效益。

(6) 北京控制与电子技术研究所：FPGA 设计信息流安全建模与形式化验证技术已集成到我单位自主研制的 FPGA 安全性分析软件中，并在多个型号产品 FPGA 代码设计安全性检测中实际应用，解决了目前 FPGA 设计安全验证手段和工具缺失的痛点问题，为关键型号产品 FPGA 设计安全检测提供有力技术支撑。

(7) 深圳市纽创信安科技开发有限公司：密码芯片设计安全验证与脆弱性检测技术已在我公司密码 IP 核和密码芯片设计安全性检测中实际应用，脆弱性检测和定位效率提升达 37%，技术水平领先，直接或间接产生数千万元的经济效益。

(8) 成都环宇芯科技有限公司：密码 IP 核设计安全形式化验证与信息泄漏检测技术已应用于我公司 HYS2210RISC-V 处理器芯片内置密码模块安全性测评业务，提升了我司处理器密码模块设计的安全性，避免因芯片安全脆弱性导致的重新设计开销和安全攻击造成的损失，具有良好的社会经济效益。

(9) 龙芯中科技股份有限公司：纳米级芯片硬件综合安全评估关键技术研究成果中的处理器集成电路设计信息流安全分析工具 V2.0 和基于形式化验证的处理器集成电路设计安全性分析工具 V2.0 已应用于我司某型国产处理器芯片设计安全性测评业务，使得所设计的处理器产品能够更好的抵御时间侧信道攻击。

(10) 北京轩宇空间科技有限公司：芯片设计安全评估技术已在我单位处理器、微处理器、存储器等产品的基础产品应用验证工作中实际应用，解决了现有设计评价检测手段只能实现等价性验证，难以发现原始设计缺陷以及复杂逻辑潜在通路的关键问题，为型号用核心芯片设计流片前安全评估提供了新技术途径和有力支撑。

六、主要知识产权和标准规范等目录（限 10 条）

序号	知识产权类别	知识产权具体名称	国家 (地区)	授权号	授权日期	证书编号	权利人	发明人
1	发明专利	一种基于信息流安全验证的硬件木马检测方法	中国	ZL201910280834.5	2022 年 04 月 05 日	第 5048611 号	西北工业大学深圳研究院，西北工业大学	胡伟，邵瑜，慕德俊
2	发明专利	基于属性自动提取和形式化验证的硬件木马搜索检测方法	中国	ZL202111511312.5	2024 年 02 月 23 日	第 6732782 号	西北工业大学	胡伟，武玲娟，李一玮，邵瑜
3	发明专利	一种基于 LUT 特征提取和机器学习的硬件木马检测方法	中国	ZL202210366564.1	2024 年 03 月 08 日	第 6771641 号	西北工业大学	武玲娟;胡伟;李一玮
4	发明专利	寄存器传输级 Verilog 代码的 SMV 模型构建方法	中国	ZL201910010500.6	2021 年 01 月 05 日	第 4192250 号	西北工业大学，华芯安信(北京)科技有限公司	沈利香，慕德俊，曹国，徐强，时翔，袁晓宇，潘群
5	发明专利	一种 RTL 硬件木马测试向量的生成方法	中国	ZL201710462372.X	2019 年 11 月 22 日	第 3606198 号	西北工业大学	沈利香，慕德俊，时翔，徐强，邢业新，何松袁晓宇
6	发明专利	一种基于门级污染标签跟踪模型的硬	中国	ZL202011147803.1	2022 年 01 月 04 日	第 4879316 号	华芯安信（北京）科技有限	慕德俊，朱岩，秦茂

		件安全漏洞检测方法					公司，西北工业大学	源，胡伟
7	论文	Theoretical Fundamentals of Gate Level Information Flow Tracking	中国	DOI: 10.1109/TCAD.2011.2120970	2011 年 07 月 11 日	IEEE Trans on Computer-Aided Design of Integrated Circuits and Systems	西北工业大学	Wei Hu, Jason Oberg, Ali Irturk, Mohit Tiwari, Timothy Sherwood, Dejun Mu, and Ryan Kastner
8	论文	Gate Level Information Flow Tracking for Security Lattices	中国	DOI: 10.1145/2676548	2014 年 11 月 18 日	ACM Transactions on Design Automation of Electronic Systems	西北工业大学	Wei Hu, Dejun Mu, Jason Oberg, Baolei Mao, Mohit Tiwari, Timothy Sherwood, and Ryan Kastner
9	论文	Hardware Information Flow Tracking	中国	DOI: 10.1145/3447867	2021 年 05 月 03 日	ACM Computing Surveys	西北工业大学	Wei Hu, Armaiti Ardeshiri cham and Ryan Kastner

10	论文	Quantitative Analysis of Timing Channel Security in Cryptographic Hardware Design	中国	DOI: 10.1109/TCAD.2017. 2768420	2018 年 09 月 01 日	IEEE Trans on Computer- Aided Design of Integrated Circuits and Systems	西北工业大学	Baolei Mao, Wei Hu, Alric Althoff, Janarbek Matai, Yu Tai, Dejun Mu, Timothy Sherwood, Ryan Kastner
----	----	---	----	---------------------------------------	------------------	--	--------	---

七、主要完成人情况

姓名	排名	行政职务	技术职称	工作单位	完成单位	对本项目贡献
胡伟	1	院长助理	教授	西北工业大学	西北工业大学	完成人全面参与了芯片安全评估技术的体系化研究及应用验证。科技创新成果 1-1：芯片设计细粒度信息流分析技术；科技创新成果 1-2：芯片设计细粒度安全建模技术；科技创新成果 2-1：融合芯片设计结构和行为特征的安全脆弱性特征提取技术；科技创新成果 3-1：芯片安全属性形式化验证方法；科技创新成果 3-2：基于属性验证的安全脆弱性搜索挖掘技术；在该项目研发工作中投入的工作量占本人工作量的 80%。
张延伟	2	部长	研究员	中国空间技术研究院	中国空间技术研究院	完成人参与了芯片设计安全建模、属性验证与脆弱性挖掘技术研究及应用验证。科技创新成果 1-2：芯片设计细粒度安全建模技术；科技创新成果 3-1：芯片安全属性形式化验证方法；科技创新成果 3-2：基于属性验证的安全脆弱性搜索挖掘技术；推动了项目成果在国产芯片设计安全性检测中的应用验证;在该项目研发工作中投入的工作量占本人工作量的 60%。

慕德俊	3	副院长	教授	西北工业大学	西北工业大学	完成人参与了芯片设计安全行为分析与建模技术和芯片设计安全脆弱性检测技术研究。科技创新成果 1-1：芯片设计细粒度信息流分析技术；科技创新成果 1-2：芯片设计细粒度安全建模技术；科技创新成果 2-2：基于智能化特征匹配的安全脆弱性检测技术；科技创新成果 3-2：基于属性验证的安全脆弱性搜索挖掘技术；在该项目研发工作中投入的工作量占本人工作量的 60%。
屈若媛	4	副主任	高级工程师	中国空间技术研究院	中国空间技术研究院	完成人参与了芯片设计安全属性验证与脆弱性搜索挖掘技术研究及应用验证。科技创新成果 3-1：芯片安全属性形式化验证方法；科技创新成果 3-2：基于属性验证的安全脆弱性搜索挖掘技术；推动了项目成果在国产芯片设计安全性检测中的应用验证；在该项目研发工作中投入的工作量占本人工作量的 40%。
武玲娟	5	/	助理研究员	西北工业大学	西北工业大学	完成人参与了芯片设计安全脆弱性特征提取与智能匹配技术研究。科技创新成果 2-1：融合芯片设计结构和行为特征的安全脆弱性特征提取技术；科技创新成果 2-2：基于智能化特征匹配的安全脆弱性检测技术；在该项目研

						发工作中投入的工作量占本人工作量的 40%。
沈利香	6	/	副教授	西北工业大学	西北工业大学	完成人参与了芯片设计安全属性验证与脆弱性搜索挖掘技术研究。科技创新成果 3-1：芯片安全属性形式化验证方法；科技创新成果 3-2：基于属性验证的安全脆弱性搜索挖掘技术；在该项目研发工作中投入的工作量占本人工作量的 30%。
邵瑜	7	/	副研究员	西北工业大学	西北工业大学	完成人参与了芯片设计安全行为分析与建模技术研究。科技创新成果 1-1：芯片设计细粒度信息流分析技术；科技创新成果 1-2：芯片设计细粒度安全建模技术；在该项目研发工作中投入的工作量占本人工作量的 30%。
毛保磊	8	/	高级实验师	西北工业大学	西北工业大学	完成人参与了芯片设计安全属性验证和脆弱性挖掘技术研究。科技创新成果 1-2：芯片设计细粒度安全建模技术；科技创新成果 3-2：基于属性验证的安全脆弱性搜索挖掘技术；在该项目研发工作中投入的工作量占本人工作量的 30%。
朱丹	9	/	副教授	西北工业大学	西北工业大学	完成人参与了芯片设计安全建模和脆弱性搜索挖掘技术研究。科技创新成果 3-2：基于属性验证的安全脆弱性搜索挖掘技术；在该项目研发工作中投

						入的工作量占本人工作量的 30%。
周慧思	10	/	副教授	西北工业大学	西北工业大学	完成人参与了芯片设计安全属性验证与脆弱性搜索挖掘技术研究。科技创新成果 3-1：芯片安全属性形式化验证方法；在该项目研发工作中投入的工作量占本人工作量的 30%。

八、主要完成单位情况及创新推广贡献

完成单位	排名	对本项目科技创新和应用推广情况的贡献 (限 600 字)
西北工业大学	1	西北工业大学研究团队经过多年的研究探索和技术攻关，突破了芯片设计安全行为分析与建模、芯片设计安全脆弱性特征提取与智能匹配和芯片设计安全属性验证与脆弱性搜索挖掘等关键技术，并开展了芯片设计安全分析工具研发与应用验证。对本项目的贡献主要体现在：作为本项目第一完成单位，全面负责项目的总体规划、设计、实施与组织，为本项目提供了大力支持和充分保障，确保了项目的顺利进行；整合项目中多类关键技术的先进优势，结合自身长期在芯片设计信息流安全分析、细粒度安全建模、脆弱性特征提取与检测等领域的研究成果，在多项核心共性基础技术上取得了突破，完成芯片设计安全脆弱性分析技术的体系化建设。上述关键技术与成果已成功应用于多个具体项目中，提高了硬件系统的安全性和可靠性，解决了传统安全防护技术无法满足硬件安全的关键问题，提高了国产硬件系统稳定性、安全性与可靠性，并产生了非常显著的经济和社会效应。
中国空间技术研究院	2	中国空间技术研究院作为本项目的合作单位，为本项目的技术研发和核心框架的建立提供了所需人员、技术成果等多方面的支持，对本项目的贡献主要体现在：通过合作立项“典型接口电路形式验证建模及遍历技术研究及试验”等项目，参与了芯片设计安全属性验证与脆弱性搜索挖掘技术研究，提出了一种芯片安全属性形式化验证方法和一种基于属性验证的安全脆弱性搜索挖掘技术；参与了芯片设计典型安全脆弱性分析和芯片安全检测总体方案设计，提出了芯片设计安全分析工具总体架构设计，并推动项目研究成果在国产芯片设计安全性检测中的应用验证，产生了显著的社会和经济效益。

九、完成人合作关系说明

完成人胡伟、郇瑜、毛保磊均参与了完成人慕德俊主持的本项目任务来源课题“基于门级信息流分析的集成电路设计安全漏洞检测技术研究”，获发明专利授权 1 项，并联合发表了多篇学术论文。完成人沈利香、慕德俊合作开展了芯片安全方面的研究，获发明专利授权 2 项。完成人武玲娟为西北工业大学博士后，合作导师为胡伟教授，共同取得授权发明专利 2 项。完成人朱丹与完成人胡伟联合开展了“密码 IP 核设计安全形式化验证与信息泄露检测技术”研究，并推动了研究技术成果的应用验证，取得了良好的应用成效。

完成人张延伟、屈若媛所在的中国空间技术研究院作为芯片设计安全检测应用推广单位，与西北工业大学有长期的合作关系。完成人胡伟、郇瑜承担了中国空间技术研究院“典型接口电路形式验证建模及遍历技术研究及试验”项目；完成人周慧思承担了中国空间技术研究院“大规模集成电路逻辑完备性建模及逻辑加强技术研究”项目。西北工业大学完成人胡伟、周慧思与中国空间技术研究院完成人张延伟、屈若媛联合开展了“芯片设计安全评估技术”研究，并推动了研究技术成果的应用验证，取得了良好的应用效果和经济效益。