项目名称：集成电路硬件安全关键技术研究

提名意见： 我单位认真审阅了该项目提名书及附件材料，确认全部材料真实有效，相关内容符合湖南省科学技术奖的提名要求。该项目系统地研究了物理不可克隆函数（PUF）、逻辑混淆、芯核（IP）水印等新型硬件安全技术，取得了国际领先的创新性学术成果：
1）深入分析 PUF 结构，发现当前主流的 RO PUF 和 Arbiter PUF 不适用于 FPGA 芯片，提出一种专用于 FPGA 的 PUF 电路结构，扩展了 PUF 在 FPGA IP 保护、软件安全和 FPGA 系统安全领域的新应用。
2）深入研究集成电路逻辑混淆技术，发现当前混淆技术用于 FPGA IP 保护时存在开销过大难以在实际电路中部署的问题，提出 “固定逻辑混淆”的反逆向工程技术，将逻辑混淆的时延开销降为零、面积开销控制在 1%左右。
3）深入研究 IP 水印技术，发现当前 IP 水印技术存在降低设计性能、产生高硬件开销且嵌入的水印在低层次难以验证等问题，提出了零开销公开可验证的 FPGA IP 水印技术。
本项目相关研究成果在 IEEE TIFS、IEEE TCAD、DAC 等国内外重要期刊和会议发表。研究成果被 IEEE Fellow、权威杂志主编、领域知名学者高度评价：“当前第一个”、“性能最优”、“以作者姓氏命名 PUF”等，在国内外产生了重要的学术影响。基于项目研究成果，第一完成人获湖南省杰出青年基金资助、入选湖湘青年英才计划。

项目简介：

该项目属于信息安全（系统安全）与集成电路技术学科交叉领域。集成电路已广泛应用于工业生产、交通运输、移动通信、金融支付等众多关系国计民生的领域，成为我国信息化体系中的重要基础。由于信息产业构建在集成电路“硬件”之上，硬件一旦存在安全问题，造成的隐患和后果十分巨大。本项目开展物理不可克隆函数（PUF）、逻辑混淆、芯核（IP）水印等新型硬件安全技术研究，取得了国际领先的创新性学术成果：

1）深入分析 PUF 结构，发现当前主流的 RO PUF 和 Arbiter PUF 不适用于 FPGA 芯片，提出一种专用于 FPGA 的 PUF 电路结构，被同行命名为“Zhang PUF”，横向对比实验显示其优于先前主流的 RO PUF、Arbiter PUF、Butterfly PUF、CD PUF 和 Anderson PUF；深入研究 PUF 应用场景，发现 PUF 应用的局限性问题，提出当前第一个非加密的 FPGA IP 保护技术。

2）深入研究集成电路逻辑混淆技术，发现当前混淆技术用于 FPGA IP 保护时存在开销过大难以在实际电路中部署的问题，提出被国际同行命名为“固定逻辑混淆”的反逆向工程技术，将逻辑混淆的时延开销降为零、面积开销控制在 1%左右。

3）深入研究 IP 水印技术，发现当前 IP 水印技术存在降低设计性能、产生高硬件开销且嵌入的水印在低层次难以验证等问题，提出了零开销可验证的 FPGA IP 水印技术，成功将 IP 保护的成本降为零。

本项目第一完成人相关研究成果（第一作者或通信作者）在 IEEE TIFS、IEEE

TCAD、DAC 等国内外重要期刊和会议发表，其中 IEEE Transactions 13 篇，获授权中国发明专利 3 项。PUF 领域发展近 20 年，第一完成人为大陆研究机构学者首次在 DAC、IEEE-TIFS 和 IEEE-TCAD 等 CCF A 类刊物发表该领域研究成果。8 篇代表性论文 WOS 他引 116 次。研究成果被 IEEE Fellow、权威杂志主编、领域知名学者高度评价：“当前第一个”、“性能最优”、“以作者姓氏命名 PUF”等，在国内外产生了重要的学术影响。基于该项目研究成果，第一完成人获湖南省杰出青年基金资助、入选湖湘青年英才计划。

客观评价：

科学发现 1 的客观评价：

中科院计算所体系结构国家重点实验室副主任、IEEE 亚太地区测试技术委员会副主席李晓维研究员在 CCF A 类顶级期刊 IEEE TCAD 论文中对代表作 1 做出高度评价：“张吉良提出使用 PUF 来保护 FPGA IP 核。该工作提供了按设备付费许可的模式来有效地帮助 IP 厂商保护他们的产品。这也是当前第一个非加密的 FPGA IP 保护思想。” [见附件 1]

清华大学周强教授在 CCF 推荐国内权威期刊论文中将申请人代表作 8 提出的 PUF 命名为“Zhang PUF”，并与当前主流的 RO PUF、仲裁器 PUF、蝴蝶 PUF、CD PUF、Anderson PUF 在唯一性和稳定性方面做了横向对比，实验结果显示其性能优于以上主流 PUF 结构。[见附件 2]

国家“百千万人才工程”国家级人选汪鹏君教授对申请者的工作多次引用并高度评价：“Zhang 等人[代表作 1]提出 PUF-FSM 的硬件混淆，有效地保护了 FPGA 器件的 IP 核，实现了 Pay-Per-Device 的强制付费许可机制”，“在应用中，PUF-FSM 硬件混淆方法有效地保护了 FPGA 器件的 IP 核，实现了按设备付费的强制支付许可功能[代表作 1]。” [见附件 3]

科学发现 2 的客观评价：

IEEE Fellow、IEEE TCAS I 主编、IEEE TVLSI 和 IEEE TSP 副主编 Keshab K. Parhi 教授对科学发现 2 进行了跟进研究，专用一章节对代表作 2 以图文的形式进行了详尽分析，将该技术命名为“fixed obfuscation”技术，并在此基础上进一步提出 dynamic obfuscation 技术，Parhi 教授的该成果发表在 CCF A 类顶级期刊 IEEE TIFS。[见附件 12]

科学发现 3 的客观评价：

YMCA University of Science and Technology 研究人员在 Multimedia Tools and Applications（IF: 2.101）期刊论文中对申请人的工作进行了高度正面评价，指出申请人提出的公开验证 IP 水印技术性能最优：“It is evident from the above Table that the technique proposed by Zhang et al. (代表作 6) is the best one…”, “this proposal (代表作 6) is the best amongst all of the watermarking techniques in the literature.” [见附件 14]

代表作及论文目录

[1] Jiliang Zhang*, Yaping Lin, Yongqiang Lyu, Gang Qu, “A PUF-FSM Binding

Scheme for FPGA IP Protection and Pay-per-Device Licensing", *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 10, no. 6, pp. 1137-1150, June 2015.

[2] Jiliang Zhang*, "A Practical Logic Obfuscation Technique for Hardware Security", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, vol. 24, no. 3, pp. 1193-1197, March 2016.

[3] Pengfei Qiu, Yongqiang Lyu, Jiliang Zhang*, et al., "Physical Unclonable Functions-based Linear Encryption against Code Reuse Attacks", in *53rd Design Automation Conference (DAC)*, Austin, USA, June 5-9 2016.

[4] Jiliang Zhang*(张吉良), Binhang Qi, Zheng Qin, Gang Qu, "HCIC: Hardware-assisted Control-flow Integrity Checking", *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 458-471, Feb. 2019.

[5] Jiliang Zhang*, Yaping Lin, Gang Qu, "Reconfigurable Binding against FPGA Replay Attacks", *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, vol. 20, no. 2, pp. 1-20, February 2015.

[6] Jiliang Zhang*, Lele Liu, "Publicly Verifiable Watermarking for Intellectual Property Protection in FPGA Design", *IEEE Transactions on Very Large Scale Integration Systems (TVLSI)*, vol. 25, no. 4, pp. 1520 – 1527, April 2017.

[7] Pengfei Qiu, Yongqiang Lv, Jiliang Zhang*, et al., "Control Flow Integrity based on Lightweight Encryption Architecture", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 37, no. 7, pp. 1358-1369, July 2018.

[8] Jiliang Zhang, Qiang Wu, Yipeng Ding, et al., "Techniques for Design and Implementation of an FPGA-specific Physical Unclonable Function", Journal of Computer Science and Technology (JCST), 31(1): 124–136, Jan. 2016

主要完成人情况

张吉良，项目负责人，是三个重要科学发现点的提出者，代表作及论文 1-2，4-6 的第一作者兼通信作者，代表作及论文 3、7 的通信作者、代表作及论文 8 的第一作者。在发现点 1 中，提出并实现了一种专用于 FPGA 的 PUF 结构；提出了一种基于 PUF 的非加密 FPGA IP 保护技术；提出并实现了基于 PUF 抵抗代码重用攻击的方法；提出并实现了一种基于 PUF 抵抗 FPGA 位流重放攻击的防御方法。在发现点 2 中，提出并实现了一种"固定逻辑混淆"的反逆向工程技术。在发现点 3 中，提出并实现了一种零开销可验证的 FPGA IP 水印技术，以及一种基于混沌的公开可验证 FPGA IP 水印检测协议。

王兴伟，第二完成人，是项目主要完成人，是代表作及论文 8 的通信作者，代表作及论文 3 的作者。在发现点 1 中设计了一种专用于 FPGA 的 PUF 结构，对抗代码重用攻击硬件体系结构进行了兼容性分析。

邱朋飞，第三完成人，是项目主要完成人，是代表作 3,7 的第一作者。在发现点 1 中提出了抗代码重用攻击的硬件体系结构。

主要完成单位情况

湖南大学为项目第一完成单位，是重要科学发现点 1、3 的提出单位，代表作及论文 1、4-6 的第一单位。在发现点 1 中，提出了一种基于 PUF 的非加密 FPGA IP 保护技术；提出了一种基于 PUF 抵抗代码重用攻击的方法；提出了一种基于 PUF 抵抗 FPGA 位流重放攻击的防御方法。在发现点 3 中，提出了一种零开销可验证的 FPGA IP 水印技术，以及一种基于混沌的公开可验证 FPGA IP 水印检测协议。

东北大学为项目第二完成单位，是重要科学发现点 2 的提出单位，代表作及论文 2、8 的第一单位。在发现点 1 中，提出了一种专用于 FPGA 的 PUF 结构。在发现点 2 中，提出了一种“固定逻辑混淆”的反逆向工程技术。

清华大学为项目第三完成单位，是重要科学发现点 1 的提出单位，是代表作 3,7 的第一单位。在发现点 1 中提出了抗代码重用攻击的硬件体系结构。

主要完成人合作关系说明

项目负责人（第一完成人）从 2011 年开始从事集成电路硬件安全技术研究。2015 年 4 月入职东北大学，与主要完成人东北大学王兴伟教授（第二完成人）同属一个研究团队，开展集成电路硬件安全技术研究，合作完成了代表作及论文 3、8。2015 年 9 月开始与清华大学吕勇强副研究员联合指导清华大学博士生邱朋飞（第三完成人）开展集成电路硬件安全技术研究，合作完成了代表作及论文 3、7。上述所有完成人共同完成了代表作 3 的研究工作，为本项目的完成做出了重要贡献。

本项目第一完成人与主要完成人均以第一作者或通信作者实质性合作完成了代表性论文，共同完成了本项目的重要科学发现点。