

## 国家自然科学基金资助项目批准通知

陈东龙 先生/女士：

根据《国家自然科学基金条例》规定和专家评审意见，国家自然科学基金委员会（以下简称自然科学基金委）决定资助您申请的项目。项目批准号：62002023，项目名称：量子安全的格密码系统软硬件协同计算平台的研究，直接费用：24.00万元，项目起止年月：2021年01月至2023年12月，有关项目的评审意见及修改意见附后。

请尽早登录科学基金网络信息系统（<https://isisn.nsfc.gov.cn>），获取《国家自然科学基金资助项目计划书》（以下简称计划书）并按要求填写。对于有修改意见的项目，请按修改意见及时调整计划书相关内容；如对修改意见有异议，须在电子版计划书报送截止日期前向相关科学处提出。

电子版计划书通过科学基金网络信息系统（<https://isisn.nsfc.gov.cn>）上传，依托单位审核后提交至自然科学基金委进行审核。审核未通过者，返回修改后再行提交；审核通过者，打印纸质版计划书（一式两份，双面打印），依托单位审核并加盖单位公章，将申请书纸质签字盖章页订在其中一份计划书之后，一并将上述材料报送至自然科学基金委项目材料接收工作组。电子版和纸质版计划书内容应当保证一致。**自然科学基金委将对申请书纸质签字盖章页进行审核，对存在问题的，允许依托单位进行一次修改或补齐。**

向自然科学基金委补交申请书纸质签字盖章页、提交和报送计划书截止时间节点如下：

1. **2020年10月14日16点**：提交电子版计划书的截止时间（视为计划书正式提交时间）；
2. **2020年10月21日16点**：提交电子修改版计划书的截止时间；
3. **2020年10月28日16点**：报送纸质版计划书（其中一份包含申请书纸质签字盖章页）的截止时间。
4. **2020年11月18日16点**：报送修改后的申请书纸质签字盖章页的截止时间。

请按照以上规定及时提交电子版计划书，并报送纸质版计划书和申请书纸质签字盖章页，未说明理由且逾期不报计划书或申请书纸质签字盖章页者，视为自动放弃接受资助；未按要求修改或逾期提交申请书纸质签字盖章页者，将视情况给予暂缓拨付经费等处理。

附件：项目评审意见及修改意见表

国家自然科学基金委员会  
2020年9月18日

附件：项目评审意见及修改意见表

项目批准号	62002023	项目负责人	陈东龙	申请代码1	F0206
项目名称	量子安全的格密码系统软硬件协同计算平台的研究				
资助类别	青年科学基金项目		亚类说明		
附注说明					
依托单位	北京师范大学-香港浸会大学联合国际学院				
直接费用	24.00 万元		起止年月	2021年01月 至 2023年12月	
<p>通讯评审意见：</p> <p>&lt;1&gt;具体评价意见：</p> <p>一、请针对创新点详细评述申请项目的创新性、科学价值以及对相关领域的潜在影响。</p> <p>该申请项目以信息安全领域为主，研究搭建后量子安全下软硬件协同的格密码专属计算平台，在如今通信系统安全日益重要的环境下十分具有前瞻性。针对云端场景下的安全需求，对格密码软硬件协同设计做出一系列的改进和研究，方法合理且创新性较强，研究成果具有较强的实用性。综合来讲，该项目立意新颖，研究支持多种主流格密码系统的计算平台，对日后我国制定后量子密码系统标准会有一定的帮助，总体的研究方案合理可行。</p> <p>二、请结合申请项目的研究方案与申请人的研究基础评述项目的可行性。</p> <p>该课题申请人长期专注格密码算法研究工作并参考大量国内外最新研究成果，针对格密码系统算法、算术算法和硬件架构提出了一系列切实可行的研究方案，通过对算法中多项式乘法的优化、元计算单元的硬件化以及RISC-V微处理器指令集的优化综合提升了计算平台的性能、通用性和扩展性，研究思路和实现方向符合科学研究的基本方法和规律。</p> <p>三、其他建议</p> <p>&lt;2&gt;具体评价意见：</p> <p>一、请针对创新点详细评述申请项目的创新性、科学价值以及对相关领域的潜在影响。</p> <p>该项目针对量子安全的格密码系统软硬件协同计算平台展开研究，具有较强的原创性和科学价值，具体体现在三个方面：（1）提出融合NTT乘法以及Toom/Karatsuba乘法的硬件协处理器结构，（2）提出可支持多个主流格密码系统计算的高通用性计算平台，（3）设计技术自主可控的安全计算平台。该项目的预期研究成果可为云端安全服务市场提供自主可控、高性能、高通用性、易扩展的计算平台。</p> <p>二、请结合申请项目的研究方案与申请人的研究基础评述项目的可行性。</p> <p>该项目研究方案论证充分，研究路线切实可行，申请人在该领域有着较好的研究积累，已在IEEE Transactions on Circuits and Systems、IEEE Transactions on Computers等优质刊物发表多篇论文，项目的整体可行性强。</p> <p>三、其他建议</p> <p>无</p> <p>&lt;3&gt;具体评价意见：</p> <p>一、请针对创新点详细评述申请项目的创新性、科学价值以及对相关领域的潜在影响。</p> <p>格密码系统能够抵抗量子攻击，是后量子密码研究的热点问题。项目针对格密码系统算法中关键算子进行优化，设计可扩展的硬件协处理器，构建自主可控的高性能软硬件协同架构。项目研究具有高的创新性和科学价值。</p> <p>二、请结合申请项目的研究方案与申请人的研究基础评述项目的可行性。</p> <p>项目研究内容和技术路线合理，方案可行，拟解决的关键科学问题和预期目标明确。申请人前期研究基础较好。鉴于上述原因，建议优先资助。</p>					

三、其他建议

修改意见：

信息科学部

2020年9月18日