2024年度国家自然科学基金“密码中的关键数学问题”专项项目指南

数学是密码学的基石，对相关数学理论的深入研究是确保密码算法安全的前提。同时，密码学也促进了数学相关领域的发展。基于量子计算的Shor算法对传统密码体制构成潜在威胁，对相关数学困难问题带来严峻挑战。后量子密码算法亟需研究和探索新型数学困难问题，发展相关算法的计算理论，创新密码设计与分析方法并推动密码学的新型应用。

为发挥国家自然科学基金对解决国家重大需求背后基础科学问题的支撑作用，国家自然科学基金委员会数学物理科学部现启动“密码中的关键数学问题”专项项目，针对密码中的数学基础理论和前沿科学问题开展研究。

一、科学目标

凝聚密码及相关领域的优势力量，围绕密码数学原理、密码设计与分析及密码学的典型应用三个方向开展系统性研究，以期在密码重大科学问题上取得突破，提升我国密码领域的创新能力。

二、拟资助研究方向和研究内容

1. 密码数学原理的创新（申请代码1选择数学物理科学部A01～A06下属代码）

计算困难问题是设计各类密码算法的基础，其数学结构、算法设计、归约问题和计算复杂性是密码数学研究的核心。本方向重点支持但不限于以下研究内容:

（1）后量子密码中计算困难问题的数学结构、复杂性、经典归约和量子归约;

（2）后量子密码基础算法，如格约化算法、格筛法、编码译码算

法等的设计与优化;

（3）基于编码的密码数学基础问题研究及攻击方法;

（4）格密码的数学基础理论;

（5）椭圆曲线同源密码的数学基础理论;

（6）面向密码的计算数论和计算代数算法设计与优化。

2. 密码设计与分析的突破（申请代码 1 选择数学物理科学部 A01～A06 下属代码）

基于相关数学问题的密码设计与分析是实现密码体制安全的关键。本方向重点支持但不限于以下研究内容:

（1）新型高效格密码公钥加密、密钥协商和数字签名;

（2）面向密码的编码方法;

（3）有限环上编码与高效实用安全多方计算;

（4）面向安全多方计算的新型秘密共享;

（5）密码函数与流密码序列设计的新型数学方法;

（6）零知识证明的数学机理。

3. 密码学的典型应用（申请代码 1 选择数学物理科学部 A01～A06 下属代码）

随着人工智能（AI）的快速发展和密态计算的广泛应用，密码和多个信息领域热点问题的交叉日益深刻。本方向重点支持但不限于以下研究内容:

（1）基于 AI 的密码分析方法;

（2）基于编码密码的 AI 安全性分析：数学理论与模型;

（3）求解有限域上不确定大型线性方程组稀疏解的 AI 方法及其在密码中的应用;

（4）基于编码的隐私信息计算与检索方案；

（5）面向密态计算的对称密码与高效算法；

（6）极端条件下信息安全的数学理论与模型。

三、资助计划

本专项项目资助期限为4年，申请书中的研究期限应填写为“2025年1月1日-2028年12月31日”。计划资助6项左右，直接费用资助强度为200万元/项左右。

四、申请要求及注意事项

（一）申请条件

1.具有承担基础研究课题的经历；

2.具有高级专业技术职务（职称）。

在站博士后研究人员、正在攻读研究生学位以及无工作单位或者所在单位不是依托单位的人员不得作为申请人进行申请。

（二）限项申请规定

1.本专项项目申请时不计入申请和承担总数范围，正式接收申请到自然科学基金委做出资助与否决定之前，以及获资助后，计入申请和承担总数范围。

2.申请人同年只能申请1项专项项目的研究项目。

3.其他限项申请要求按照《2024年度国家自然科学基金项目指南》“限项申请规定”执行。

（三）申请注意事项

1.专项项目实行无纸化申请。申请书提交时间为2024年10月22日~10月28日16时。

2.申请人注意事项

（1）申请人在填报申请书前，应当认真阅读本申请须知、本项目指南和《2024 年度国家自然科学基金项目指南》的相关内容，不符合项目指南和相关要求的申请项目不予受理。

（2）本专项项目旨在紧密围绕核心科学问题，集中国内优势研究团队进行研究，成为一个专项项目群。申请人应根据本专项项目拟解决的具体科学问题和项目指南公布的拟资助研究方向，自行拟定项目名称、科学目标、研究内容、关键科学问题、技术路线和相应的研究经费等。

（3）申请人登录科学基金网络信息系统 https://grants.nsfc.gov.cn/（没有系统账号的申请人请向依托单位基金管理联系人申请开户），按照撰写提纲及相关要求撰写申请书。

（4）申请书中的资助类别选择“专项项目”，亚类说明选择“研究项目”，附注说明选择“科学部综合研究项目”，申请代码 1 应当按照拟资助研究方向后标明的代码要求选择数学物理科学部的申请代码。以上选择不准确或未选择的项目申请将不予受理。

（5）请按照“专项项目-研究项目申请书撰写提纲”撰写申请书。申请书正文开头注明“密码中的关键数学问题”之研究方向：XXX（按照上述 3 个研究方向之一填写）。

申请书应突出有限目标和重点突破，明确对实现本专项项目总体科学目标和解决核心科学问题的贡献。

如果申请人已经承担与本专项项目相关的其他科技计划项目，应当在申请书正文的“研究基础与工作条件”部分论述申请项目与其他相关项目的区别与联系。

（6）申请人应当严格按照《国家自然科学基金资助项目资金管理办法》等相关规定和《国家自然科学基金项目资金预算表编制说明》的具体要求，认真如实编报项目预算。

3.依托单位注意事项

（1）依托单位应对本单位申请人所提交申请材料的真实性、完整性和合规性进行审核；对申请人编制预算的目标相关性、政策相符性和经济合理性进行审核。

（2）应在规定的项目申请截止日期前通过信息系统逐项确认提交本单位电子申请书及附件材料，无需报送纸质申请书。项目获批准后，将申请书的纸质签字盖章页装订在《资助项目计划书》最后，一并提交。签字盖章的信息应与电子申请书严格保持一致。

（3）如依托单位在2024年度未上传过《2024年度国家自然科学基金项目申请承诺书》（以下简称《承诺书》），应从信息系统中下载《承诺书》，由法定代表人亲笔签名并加盖依托单位公章后，将电子扫描件上传至信息系统（本年度只需上传一次）。依托单位完成上述承诺程序后方可提交申请。

（4）依托单位在项目申请截止时间后24小时内，通过信息系统在线提交本单位项目申请清单。清单提交后，自然科学基金委方可接收项目申请材料。

4.本专项项目咨询方式:

国家自然科学基金委员会数学物理科学部

联系人：赵桂萍

联系电话：010-62327191

（四）其他注意事项

1.为实现专项项目总体科学目标，获得资助的项目负责人应当在项目执行过程中关注与本专项其他项目之间的相互支撑关系。

2.为加强项目之间的学术交流，本专项项目群将设专项项目总体指导组和管理协调组，并将不定期地组织相关领域的学术研讨会。获资助项目负责人必须参加上述学术交流活动，并认真开展学术交流。