安徽省科学技术奖提名项目公示

（2024 年度）

自然科学奖

项目名称：性能良好密码函数的刻画与构造研究

提名者：安徽财经大学

提名意见：该项目围绕性能良好密码函数的刻画与构造展开，取得了一系列特色鲜明的创新成果：1. 给出了一个 Bent 函数和向量 Bent 函数的一般化构造，极大统一了文献中许多已有 Bent 函数的构造，得到了一批性能良好的 Bent 函数和向量 Bent 函数，相关结果覆盖了至少 18 篇高质量期刊论文主要结论，回答了 Bent 函数研究方向的 2 个公开问题，深刻揭示了许多已有单变量 Bent 函数与 Maiorana-McFarland 完全类间的关系；2. 在国际上首次提出利用向量布尔函数构造性能良好极小线性码的想法，理论上完全刻画了设计极小线性码所需向量布尔函数满足的条件，得到了维数更大、性能更优的极小线性码；3. 理论上对 Bent-negabent 函数和广义布尔函数的相关函数进行了刻画与计算；4. 通过建立 CCZ-等价型，给出了性能良好的 Bent 函数，Plateaued 函数、4-差分置换等性能良好密码函数。在国内外权威期刊发表论文 20 余篇，研究成果有力推动了密码函数和极小线性码的研究进展。项目组成员立项了多项国家级项目和 1 项中国博士后面上资助，荣获了 2024 年安徽省青年数学奖和安徽省应用数学成果奖等重要奖项。

我单位认真审阅了该项目申报材料，确认全部材料真实有效，相关栏目均符合填写要求，按照要求对该项目基本情况进行了公示，目前无异议。

提名该项目为安徽省自然科学奖 二 等奖。

项目简介：性能良好的密码函数在密码学、编码理论和组合设计等学科中均有十分重要的应用。然而，人们对绝大多数密码函数的认识还不够深入、对许多已有密码函数的结构以及彼此间的关系仍不清楚，部分密码函数的高效构造成果依然较少，很多已有密码函数的研究并不彻底。因此，性能良好密码函数的刻画与构造一直是密码函数研究领域的经典课题。本项目围绕着性能良好的 Bent 函数、向量 Bent 函数、Plateaued 函数、极小线性码、4-差分置换、Bent-negabent 函数和广义布尔函数的相关函数的刻画与构造展开，取得了以下 5 方面特色鲜明的创

新性成果：

1. **在 Bent 函数和向量 Bent 函数的研究方面**，给出了一个 Bent 函数和向量 Bent 函数的一般化构造，极大统一了文献中许多 Bent 函数的构造，得到了一大批性代数次数可以任意控制的显式 Bent 函数和向量 Bent 函数并确定了相应函数的显示对偶，研究成果覆盖了至少 18 篇高质量期刊论文主要结论，回答了 Bent 函数研究方向长期存在的 2 个公开问题，给出了一大类非 Maiorana-McFarland 完全类 Bent 函数，深刻揭示了许多已有单变量 Bent 函数与 Maiorana-McFarland 完全类间的关系。

2. **在极小线性码的研究方面**，首次提出用向量布尔函数构造极小线性码的想法，在理论上完全刻画了一大类由向量布尔函数得到的线性码是性能良好极小码所需向量布尔函数满足的条件，给出了许多维数较高、极小距离较大的 3-重极小线性码和许多维数较高、极小距离较大的不满足 AB 条件的极小线性码。

3. **在 Bent-negabent 函数研究方面**，给出了一类二次布尔函数 Bent-negabent 函数的充要条件，得到了推广的 Nega-卷积定理 Nega-组合定理、以及一类非直和构造的 Nega-Hadamard 变换表示及其为 Negabent 函数的充分条件。

4. **在广义布尔函数的相关函数研究方面**，计算了一类广义布尔函数的相关函数，建立了广义布尔函数和布尔函数之间相关函数的联系。

5. **在其他密码函数研究方面**，通过建立两个一般的 CCZ-等价型，给出了性能良好的 Bent 函数，具有最大 Bent 分支的向量函数，向量 Bent 函数，具有单一振幅的向量 Plateaued 函数和三次 4-差分置换。

本项目系统研究了一系列性能良好的密码函数的刻画与构造，在《IEEE Trans. Inf. Theory》和《电子学报》等国内外权威期刊发表高质量论文 20 余篇，包括 18 篇 SCI 论文，其中 4 篇论文发表在密码与信息论旗舰期刊《IEEE Trans. Inf. Theory》上。国内外专家欧阳毅、胡红钢、屈龙江、李康荃、付方伟、曾祥勇、李念、张凤荣、Enes Pasalic、Amar Bapic、Aleksandr Kutsenko、Kaleyski Nikolay 等引用了我们的成果并给予了高度评价。在项目成果支持下，第一完成人李彦君先后立项了国家自然科学基金青年项目和中国博士后科学基金面上资助，获得了 2024 年度安徽省青年数学奖和安徽省应用数学成果三等奖。

代表性论文专著：

1. Generic constructions of (Boolean and vectorial) bent functions and their consequences. IEEE Transactions on Information Theory, 2022.
2. Minimal binary linear codes from vectorial Boolean functions. IEEE

Transactions on Information Theory, 2023.

3. Cryptographic Functions with Interesting Properties from CCZ-equivalence. Cryptography and Communications, 2023.
4. Characterization and properties of bent-negabent functions. Chinese Journal of Electronics, 2022.
5. 一类广义布尔函数的相关函数分析. 电子学报, 2019.

主要完成人情况：

李彦君，本项目第一完成人，现为安徽财经大学特聘教授，硕士生导师。 复旦大学博士后，导师阚海斌教授。主要从事密码函数的研究工作。主持国家自然科学基金青年项目、中国博士后科学基金面上项目和安徽省高校自然科学重点项目。荣获 2024 年度安徽省青年数学奖和安徽省应用数学成果奖。主要科学进展包括：1）构造了一批性能良好的 Bent 函数、Plateaued 函数、向量 Bent 函数、向量 Plateaued 函数；2）在国际上首次提出利用向量函数构造极小线性码的想法，获得了性能良好的极小线性码；3）解决了密码函数研究领域的几个公开问题，推动了密码函数的研究进展。负责本项目技术路线、研究目标和研究内容的制定，对项目的实施和完成起关键性作用，是“重要科学发现 1、2、3”的主要完成者，全程参与了重要科学发现的 1、2、3 的全部研究，是本项目代表性论文 1、2、3 的第一作者。

卓泽朋，本项目第二完成人，现为淮北师范大学数学与统计学院院长，教授。在本项目中同第五完成人杨志耀一起给出了 Bent-negabent 函数和 Negabent 函数的新刻画、推广的 Nega-卷积定理和 Nega-组合定理、一类非直和构造的 Nega-Hadamard 变换表示及其为 Negabent 函数的充分条件，计算了一类广义布尔函数的相关函数，建立了广义布尔函数和布尔函数之间相关函数的联系，研究成果为进一步研究 Negabent 函数性质与构造提供新思路，可用于判断所得广义序列的相关性，从而设计出满足低相关值的多元序列。是本项目“重要科学发现 4 和 5”的主要完成者，也是本项目代表性论文 4 和 5 的通讯作者。

阚海斌，本项目第三完成人，现为复旦大学二级教授、复旦大学特聘教授、复旦大学博士生导师、复旦大学发展规划处副处长、上海市区块链工程技术中心主任。主要从事密码函数、区块链等的研究工作，发表了一百多篇论文。以第一完成人获得了教育部自然科学二等奖 2 次，上海市科技进步一等奖 1 次，上海市自然科学二等奖 1 次，党政机要密码科技进步奖三等奖 1 次。完成了 1 项国家重

点研发计划和多项国家自然科学基金项目。培养了一批优秀的硕士和博士研究生。在本项目中，指导了一系列性能良好密码函数的刻画与构造研究，其中包括性能良好的 Bent 函数、向量 Bent 函数、Plateaued 函数、极小线性码和置换多项式等。是本项目“重要科学发现 1、2、3”的重要贡献者，给出了 Bent 函数研究的指导思想，给出了一类不满足 AB 条件的极小线性码和一类具有最大 Bent 分支的向量函数，是本项目代表性论文 1、2、3 的共同作者。

彭杰，本项目第四完成人，现为上海师范大学教授。主要从事密码函数和线性码的研究工作。主持并结项了国家自然科学基金青年项目和面上项目。以第三完成人荣获了 2024 年安徽省应用数学成果奖三等奖。培养了一批优秀的博士和硕士研究生。在本项目中，指导了一系列性能良好密码函数的刻画与构造研究，其中包括性能良好的 Bent 函数、向量 Bent 函数、Plateaued 函数、极小线性码和置换多项式等，为极小线性码和 CCZ-等价的研究提供了重要的指导思想，给出了一类 Bent 函数的对偶，两类向量 Bent 函数，一类不满足 AB 条件的极小线性码和一类 4-差分置换，是本项目“重要科学发现 1、2、3”的重要贡献者，代表性论文 2 和 3 的通讯作者，代表性论文 1 的共同作者。

杨志耀，本项目第五完成人，现为淮北师范大学数学与统计学院教师。主要从事密码函数的研究工作，在《中国科学：数学》《电子学报》等高质量期刊上发表了一系高质量期刊论文。在本项目中同第二完成人卓泽朋一起给出了 Bent-negabent 函数和 Negabent 函数的新刻画、推广的 Nega-卷积定理和 Nega-组合定理、一类非直和构造的 Nega-Hadamard 变换表示及其为 Negabent 函数的充分条件，计算了一类广义布尔函数的相关函数，建立了广义布尔函数和布尔函数之间相关函数的联系，研究成果为进一步研究 Negabent 函数性质与构造提供新思路，可用于判断所得广义序列的相关性，从而设计出满足低相关值的多元序列。是本项目“重要科学发现 4、5”中的主要完成者，代表性论文 4 的共同作者，代表性论文 5 的第一作者。

主要完成单位：

安徽财经大学，淮北师范大学，复旦大学，上海师范大学

完成人合作说明：

本项目完成人及排序为：李彦君，卓泽朋，阚海斌，彭杰，杨志耀。

本项目完成单位有四个，分别为：安徽财经大学，淮北师范大学，复旦大学

和上海师范大学。其中，李彦君的工作单位为安徽财经大学，卓泽朋和杨志耀的工作单位为淮北师范大学，阚海斌的工作单位为复旦大学，彭杰的工作单位为上海师范大学。

合作关系如下：

2017 年 9 月-2021 年 6 月，李彦君在阚海斌教授和彭杰教授的联合指导下在上海师范大学攻读博士学位，开始从事密码函数的构造研究。在此期间，李彦君、阚海斌和彭杰等构造了一些性能良好的密码函数，包括性能良好的 Bent 函数，具有较高非线性度较低绝对值指标的平衡函数，具有最大 Bent 分支的向量函数等；合作发表了 5 篇 SCI 论文，彭杰和李彦君等共同立项了国家自然科学基金面上项目一项，项目编号 61972258。**2021 年 6 月-2023 年 5 月**，李彦君在安徽财经大学任教，深入研究密码函数的刻画与构造。在此期间，李彦君、阚海斌和彭杰等刻画了一些 Bent 函数和 APN 函数的结构，给出了一些性能良好的 Bent 函数、向量 Bent 函数和 APN 函数，发表了 4 篇 SCI 论文（包括代表性论文 1）。**2023 年 5 月至 2025 年 6 月**，李彦君在阚海斌教授指导下在复旦大学读在职博士后，继续深入研究性能良好密码函数和线性码的刻画与构造。在此期间，李彦君、阚海斌和彭杰等合作发表了 8 篇 SCI 论文，包括本项目的代表性论文 2 和 3。在阚海斌教授和彭杰教授的指导下，李彦君立项了国家自然科学基金青年项目，项目编号 62302001，和中国博士后科学基金面上资助，项目编号 2023M740714。

2017 年 9 月-2020 年 6 月，杨志耀在卓泽朋教授指导下在淮北师范大学攻读硕士学位，从事性能良好密码函数的刻画与构造研究。在此期间，杨志耀和卓泽朋等合作发表了 3 篇中文论文，其中包括代表性论文 5。**2020 年 7 月-2023 年 5 月**，杨志耀和卓泽朋等合作发表了代表性论文 4。**2023 年 6 月至 2025 年 6 月**，杨志耀在淮北师范大学任教，和卓泽朋等在《密码学报》合作发表了 1 篇关于线性码的中文论文。

完成人合作关系情况汇总表

序号	合作方式	合作者	合作时间	合作成果	证明材料	备注
1	论文合著	李彦君，阚海斌，彭杰	2021年6月至2023年5月	Generic constructions of (Boolean and vectorial) bent functions and their consequences	代表性论文1	
2	论文合著	李彦君，彭杰，阚海斌	2021年6月至2023年7月	Minimal binary linear codes from vectorial Boolean functions	代表性论文2	
3	论文合著	李彦君，阚海斌，彭杰	2017年9月至2023年7月	Cryptographic Functions with Interesting Properties from CCZ-equivalence	代表性论文3	
4	论文合著	杨志耀，卓泽朋	2020年6月至2023年5月	Characterization and properties of bent-negabent functions	代表性论文4	
5	论文合著	杨志耀，卓泽朋	2017年9月至2020年6月	一类广义布尔函数的相关函数分析	代表性论文5	