编号	

安徽省青年数学奖申请表

申请人姓名　　李彦君

申请人工作单位　　安徽财经大学

申请人研究领域　　代数编码与密码

填　表　日　期　　2024 年 6 月 30 日

安徽省数学会

申请人情况简介

<table>
<tr><td>姓名</td><td>李彦君</td><td>性别</td><td>男</td><td>出生年月</td><td>1990 年 3 月</td><td>民族</td><td>汉</td></tr>
<tr><td>学位</td><td>博士</td><td>职称</td><td>特聘教授</td><td>主要研究领域</td><td colspan="3">代数编码与密码</td></tr>
<tr><td>电话</td><td colspan="3">18153958770</td><td>Email</td><td colspan="3">yanjlmath90@163.com</td></tr>
<tr><td>Fax</td><td colspan="3"></td><td>个人网页</td><td colspan="3"></td></tr>
<tr><td>工作单位</td><td colspan="7">安徽财经大学统计与应用数学学院</td></tr>
<tr><td>个人简历</td><td colspan="7">1.教育经历
2017.09-2021.06 上海师范大学，基础数学，博士，导师：阚海斌教授
2014.09-2017.06 兰州理工大学，应用数学，硕士，导师：杨胜良教授
2010.09-2014.06 天水师范学院，数学与应用数学，学士
2.工作经历
2021.06-2022.09 安徽财经大学，统计与应用数学学院，讲师
2022.09-2024.05 安徽财经大学，统计与应用数学学院，(特聘)副教授
2024.05-至今 安徽财经大学，统计与应用数学学院，(特聘)教授
2021.09-至今 安徽财经大学，龙湖学者，研究生导师
2023.05-至今 复旦大学，计算机学院，博士后，导师：阚海斌教授
3.访问经历
2019.09-2020.08 新加坡国立大学，访问学者，导师：Chik How Tan 教授
4.学术兼职
美国数学会《数学评论》评论员</td></tr>
<tr><td>获奖情况</td><td colspan="7">1. 2024 年安徽财经大学优秀教师
2. 2022 年指导全国大学生数学建模竞赛安徽省赛区三等奖
3. 2021 年上海师范大学优秀博士学位论文</td></tr>
</table>

主持的研究项目及主要学术成就简介	（不超过 2000 字） **一 主持的科研项目** 1. 国家自然科学基金，青年项目，62302001，两类新型密码函数的设计及其应用，2024-01-01 至 2026-12-31,在研 2. 中国博士后科学基金，第 74 批面上项目，2023M740714，Bent 函数的构造及其在设计平衡函数中的应用，2023-11-27 至 2025-09-01，在研 3. 安徽省高校科研计划项目，重点项目，2023AH050250，性质优良的密码函数的构造研究，2023-05-15 至 2025-05-15，在研 **二 主要学术成就简介** 申请人一直致力于性能良好的密码函数（比如 Bent 函数：抵抗线性攻击最好的密码函数，APN 函数：抵抗差分攻击最好的密码函数）和线性码的构造及其应用研究，得到了一批有意义的研究成果，解决了密码函数研究领域的几个公开问题，发表了一系列（17 篇）影响重大的高质量 SCI 检索论文；研究成果极大地推动了密码函数和线性码的研究进展，受到了密码函数和线性码研究领域国内外专家的高度认可，具有重要的理论意义和实用价值。现将论文的发表情况及学术贡献简要如下： 1. **以第一作者在信息论顶级期刊《IEEE Transactions on Information Theory》上发表关于 Bent 函数的学术论文一篇**。该论文极大地统一了以前 Bent 函数的许多构造，得到了许多性能优良的 Bent 函数和向量 Bent 函数，**正面回答了国际著名密码、编码学家 Claude Carlet 关于幂等 Bent 函数的公开问题，部分解决了 Natalia Tokareva 提出的公开问题：**什么样的布尔函数可以写成两个 Bent 函数之和，**副主编 Claude Carlet 对该论文给予了较高的评价**：. . . to get bent functions in univariate representation through Theorem 3, only one condition (based on the nullity of a second derivative) is required, which is dramatically simple compared to almost all the previous known constructions proposed in this context, . . . I believe then that this paper generalizing 17 articles published in high standard journals is worth being published in IEEE Transactions on IT; 2. **以第一作者在信息论顶级期刊《IEEE Transactions on Information Theory》上发表关于极小线性码的学术论文一篇**。该论文在国际上首次提出用向量函数构造违反 AB 条件的极小线性码，在理论上完全刻画了一类由向量函数得到的线性码是违反 AB 条件的极小线性码所需条件，并给出

了 3 类的违反 AB 条件的极小线性码。同以前得到的违反 AB 条件的极小线性码相比，该论文得到的极小线性码维数更大、性能更优。**申请人受邀在中国工业与应用数学学会第二十届年会（CSIAM 2022）上对该论文的部分结果作了汇报**，研究结论得到了会议主持人唐春明教授的肯定。

3. **在信息论顶级期刊《IEEE Transactions on Information Theory》上发表关于 APN 函数的学术论文一篇**。该论文提出了一个构造 APN 函数的新型框架，在此框架下，得到了新的无限类 APN 函数。

4. **以第一作者在国际著名期刊《Cryptography and Communications》上发表性质优良的密码函数构造的学术论文一篇**。该论文得到了两个一般的 CCZ-等价型，并据此构造了新的 Bent 函数、具有最大 Bent 分支数的向量函数、Plateaued 函数及 4 差分置换，**解决了著名密码、编码学家 Claude Carlet 关于 Pleteaued 函数的一个公开问题。申请人受邀在第七届编码密码组合国际研讨会上汇报了该论文的结论。**

5. **以第一作者在国际知名期刊《Information Processing Letters》上发表关于 Bent 函数的学术论文一篇**。该论文构造了一类新的向量 Bent 函数，**解决了国际著名密码、编码学家 Sihem Mesnager 在《IEEE Transactions on Information Theory》上提出的关于 Bent 函数的一个长达 6 年的公开问题**。

6. 除了以上重要研究成果外，申请人还在国际著名期刊《Designs, Codes and Cryptography》，《Finite Fields and Their Applications》，《Cryptography and Communications》，《Advances in Mathematics of Communications》，《IET Information Security》等上发表了一系列关于置换多项式、Bent 函数，GAPN 函数的学术论文，这些成果推动了密码函数的研究进展。

部分已发表 SCI 论文如下：

[1] **Yanjun Li,** Haibin Kan, Sihem Mesnager, Jie Peng, Chik How Tan, Lijing Zheng, Generic constructions of (Boolean and vectorial) bent functions and their consequences, IEEE Transactions on Information Theory, 2022，vol. 68, no. 4, pp. 2735-2751 (信息论顶级期刊)

[2] **Yanjun Li,** Jie Peng, Haibin Kan, Lijing Zheng, Minimal Binary Linear Codes from Vectorial Boolean Functions，IEEE Transactions on Information Theory, 2023, vol. 69, no. 5, pp. 2955-2968 (信息论顶级期刊)

[3] Lijing Zheng, Haibin Kan, **Yanjun Li,** Jie Peng, Deng Tang, Constructing New APN Functions Through Relative Trace Functions, IEEE Transactions on Information Theory, 2022，vol. 68, no. 11, pp. 7528-7537 (信息论顶级期刊)

[4] **Yanjun Li,** Haibin Kan, Jie Peng, Lijing Zheng, Cryptographic Functions with Interesting Properties from CCZ-equivalence, Cryptography and Communications，2023, vol. 15, pp. 831–844

[5] **Yanjun Li,** Jie Peng, Chik How Tan, An answer to an open problem of Mesnager on bent functions, Information Processing Letters, 2020, 161, 105974

[6] **Yanjun Li,** Jie Peng, Chik How Tan, Haibin Kan, Lijing Zheng, Further constructions of bent functions and their duals, IET Information Security, 2021, vol. 15, no. 1, pp. 87-97

[7] Changhui Chen, Haibin Kan, **Yanjun Li,** Jie Peng, Lijing Zheng, Several classes of permutation polynomials of the form $(x^{p^m}-x+\delta)^s+L(x)$, Advances in Mathematics of Communications, 2024, Early Access (通讯作者)

[8] **Yanjun Li,** Haibin Kan, Jie Peng, Chik How Tan, Baixiang Liu, The Explicit Dual of Leander's Monomial Bent Function, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021, vol. E104, pp. 1357-1360

[9] **Yanjun Li**; Haibin Kan; Jie Peng; Chik How Tan; Baixiang Liu; A New 10-variable Cubic Bent Function Outside The Completed Mariorana-McFarland Class, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2021, vol. E104, pp. 1353-1356

[10] Lijing Zheng, Jie Peng, Haibin Kan, **Yanjun Li**, Juan Luo, On constructions and properties of (n, m)-functions with maximal number of bent components, Designs, Codes and Cryptography, 2020, vol.88, pp. 2171-2186

[11] Lijing Zheng, Jie Peng, Haibin Kan, **Yanjun Li**, Several new infinite families of bent functions via second order derivatives, Cryptography and Communications, 2020, vol.12, pp.1143–1160

[12] Lijing Zheng, Haibin Kan, Tongliang Zhang, Jie Peng, **Yanjun Li**, Two classes of permutation trinomials over Fq3 in characteristic two. Finite Fields and Their Applications, 2024, 94, 102354

部分正在审稿论文如下：

[1] **Yanjun Li**, Haibin Kan, Sihem Mesnager, Jie Peng, Lijing Zheng, Direct Approaches for Generic Constructions of Plateaued Functions and Bent Functions Outside M, IEEE Transactions on Information Theory, **Minor revision**, (Sihem Mesnager 受邀在 2024 年序列及其应用(SETA2024)国际学术会议上汇报了该论文的部分结论)

代表性论文目录及引用情况	三篇代表作及引用情况 [1] **Yanjun Li,** Haibin Kan, Sihem Mesnager, Jie Peng, Chik How Tan, Lijing Zheng, Generic constructions of (Boolean and vectorial) bent functions and their consequences, IEEE Transactions on Information Theory, 2022，vol. 68, no. 4, pp. 2735-2751 (信息论顶级期刊，被引用 16 次) [2] **Yanjun Li,** Jie Peng, Haibin Kan, Lijing Zheng, Minimal Binary Linear Codes from Vectorial Boolean Functions， IEEE Transactions on Information Theory, 2023, vol. 69, no. 5, pp. 2955-2968 (信息论顶级期刊，被引用 1 次) [3] Lijing Zheng, Haibin Kan, **Yanjun Li,** Jie Peng, Deng Tang, Constructing New APN Functions Through Relative Trace Functions, IEEE Transactions on Information Theory, 2022，vol. 68, no. 11, pp. 7528-7537 (信息论顶级期刊，被引用 11 次)

推荐人推荐意见

被推荐人的原创性学术成果，已有的应用成果或可能的应用前景(包括代表性著作、论文、专利或成果鉴定等)：

尊敬的安徽省青年数学奖评审委员会：

李彦君博士是我在上海师范大学指导的博士研究生，现在他跟着我读复旦大学的在职博士后。他具有扎实的数学功底，做事勤奋认真，在密码函数和线性码的研究领域发表了一系列具有很强影响力的学术论文。我们合作的一篇关于 Bent 函数的论文统一了 17 篇发表在《IEEE Transactions on Information Theory》，《Designs, Codes and Cryptography》，《Science China Information Sciences》等著名期刊上的高质量论文结果；解决了国际著名密码、编码学家 Claude Carlet 和 Sihem Mesnager 关于 Bent 函数的两个公开问题，解决了 Claude Carlet 关于 Plateaued 函数的一个公开问题，部分解决了 Natalia Tokareva 关于 Bent 函数的一个公开问题；在国际上我们首次利用向量布尔函数构造违反 AB 条件的极小线性码，得到了维数更大、性能更优的违反 AB 条件的极小线性码。这些研究成果极大地推动了密码函数和极小线性码的研究进展，为对称密码设计提供了良好的函数选择；此外，他还主持国家自然科学基金青年项目和中国博士后科学基金面上项目各一项。

综上，李彦君博士得到了一批具有重要意义的研究成果，具有很强的科研潜力。因此，我强烈推荐他申报 2024 年“安徽省青年数学奖”。

推荐人签名：

2024 年 7 月 2 日

推荐人工作单位：复旦大学
推荐人通讯地址：上海市复旦大学江湾校区计算机学院
邮政编码：200433
推荐人联系电话：　　(O)，　　(H)，手机：13162736845
推荐人 Email Address:hbkan@fudan.edu.cn
推荐人 Fax # ：

推荐人推荐意见

被推荐人的原创性学术成果，已有的应用成果或可能的应用前景(包括代表性著作、论文、专利或成果鉴定等)：

尊敬的安徽省青年数学奖评审委员会：

李彦君博士现在是安徽财经大学的特聘教授，研究生导师，龙湖学者。他的主要研究方向为密码学和编码学。他和合作者构造了一批新的具有优良密码性质的密码函数，比如 Bent 函数和 APN 函数，解决了密码函数研究领域的几个公开问题，研究成果极大地促进了密码函数的研究进展。此外，李彦君博士及其合作者在极小线性码的研究方面也得到了很好的研究成果：他们首次提出利用向量布尔函数构造不满足 AB 条件的极小线性码，根据这一创新性的想法，他们得到维数更大、性能更优的极小线性码，研究成果用在秘密共享中可使其具有良好的接入结构，用在安全双方计算中可确保隐私安全。

李彦君博士与国内外专家积极互动。他曾受邀在中国工业与应用数学学会第二十届年会和第七届编码密码组合国际研讨会上汇报过他们团队的科研成果，受到了与会专家的高度肯定。他也多次邀请同行专家讨论交流、给安徽财经大学师生作学术报告。他还与国际密码、编码学家 Sihem Mesnager 和 Chik How Tan 有密切的合作，其合作论文发表在国际信息论顶级期刊《IEEE Transactions on Information Theory》上。

鉴于上述李彦君博士在科研上的巨大潜力和突出表现，我大力推荐他申报 2024 年“安徽省青年数学奖”。

推荐人签名：

2024 年 7 月 3 日

推荐人工作单位：合肥工业大学数学学院
推荐人通讯地址：安徽省合肥市蜀山区翡翠路420
邮政编码：230601
推荐人联系电话：　　(O)，　　(H)，手机：13505600105
推荐人 Email Address: zhushixin@hfut.edu
推荐人 Fax # ：

评奖委员会意见	签字： 年　月　日
备注	