# 2022 年编码与密码及相关数学理论国际研讨会

# 2022 International Workshop on Coding Theory & Cryptography and Related Mathematical Theory

# 会议手册

福建师范大学数学与统计学院
福建省数学联盟
莆田学院数学与金融学院
2022 年 12 月 3 日—4 日

# 目录

一、会议通知.....1

二、会议日程.....3

三、报告简介.....4

四、通讯录.....10

五、附录

学院简介.....11

会议记录.....12

# 2022 年编码与密码及相关数学理论国际研讨会

2022 International Workshop on Coding Theory & Cryptography and Related Mathematical Theory

# 会议通知

为促进编码与密码领域学者的交流与合作，2022 年编码与密码及相关数学理论国际研讨会（2022 International Workshop on Coding Theory & Cryptography and Related Mathematical Theory）将于 2022 年 12 月 3 日—4 日在福建福州举行。鉴于当前疫情形势，本次会议将全程线上参会。本次会议由福建师范大学数学与统计学院、福建省数学联盟主办，莆田学院数学与金融学院协办。会议旨在为从事密码、编码以及信息安全研究的广大青年学者、技术人员和在校研究生提供学术交流合作平台。会议将邀请编码、密码学与信息安全等研究领域的专家学者做特邀报告。诚邀数学、密码及信息安全领域广大学者、业界精英、工程技术人员、管理人员和在校研究生参会。现将会议有关事项通知如下：

**一、主办单位：**福建师范大学数学与统计学院

福建省数学联盟

**二、协办单位：**莆田学院数学与金融学院

**三、会议时间：**2022 年 12 月 3—4 日

**四、会议方式：**腾讯会议（ID: 859-5245-2302）

**注：技术原因，3 日下午俄罗斯 Vladimir Edemskiy 报告，Zoom 会议，Meeting ID: 926 0822 1724. Password: NW9XK6，链接如下：https://zoom.us/j/92608221724?pwd=MDFYdGlFcGRWN25iSWhrQUtNVjFpdz09**

**五、会务组及联系方式：**

柯品惠 keph@fjnu.edu.cn, 林昌露 cllin@fjnu.edu.cn, 陈智雄 ptczx@126.com
赵晨阳 zcy1320@126.com，13205038997

福建师范大学数学与统计学院

2022 年 11 月 12 日

# 会议日程

| 2022 年 12 月 3 日（星期六）（腾讯会议：859-5245-2302） | | | |
|---|---|---|---|
| 时间 | 内容 | | 主持人 |
| | 报告人 | 报告题目 | |
| 8:20-8:30 | 开幕式 | | 柯品惠 |
| 8:30-9:30 | Huaxiong Wang<br>（新加坡南洋理工大学） | Combinatorial Cryptography | 林昌露 |
| 9:30-10:30 | Lein Harn<br>（美国密苏里大学） | My Recent Research on Secret Sharing: Key Distribution and Group Authentication | |
| 10:30-11:30 | 赖俊祚<br>（暨南大学） | 选择打开安全的公钥加密 | |
| 11:30-14:00 | 午餐、午休 | | |
| 14:00-15:00 | Vladimir Edemskiy<br>（俄罗斯诺夫哥罗德国立大学） | The 4-adic complexity of generalized cyclotomic quaternary sequences with a period of $2p^m$ | 陈智雄 |
| 15:00-16:00 | 施敏加<br>（安徽大学） | Equivalence and Duality of Polycyclic Codes Associated with Trinomials over Finite Fields | |
| 16:00-17:00 | Chunlei Li<br>（挪威卑尔根大学） | On decoding of rank-metric codes | |
| 17:00-18:00 | 夏永波<br>（中南民族大学） | More Properties about A Family of Ternary Almost Perfect Nonlinear Mappings | |

| 2022 年 12 月 4 日（星期日）上午（腾讯会议：859-5245-2302） | | | |
|---|---|---|---|
| 时间 | 内容 | | 主持人 |
| | 报告人 | 报告题目 | |
| 9:00-10:00 | 常祖领<br>（郑州大学） | $k$-置换广义圈的计数与构造<br>（Enumerations and Constructions of Universal Cycles for $k$-permutations） | 柯品惠 |
| 10:00-11:00 | 程航<br>（福州大学） | 基于外包加密监控视频的安全可验证行人再识别技术 | |
| 11:00-12:00 | 祝辉林<br>（厦门大学） | Some Time-Asymmetric Encoding Schemes Based on $N$-th Root and Discrete Logarithm Problem over a Finite Field | |

# 报告简介

| | |
|---|---|
| 报告专家 | Huaxiong Wang（新加坡南洋理工大学） |
| 报告题目 | Combinatorial Cryptography |
| 报告摘要 | Combinatorics has been playing an active role in cryptography, from the designs of cryptographic constructions, security proofs to cryptanalysis. Combinatorial cryptography refers to a sub-field of cryptography where combinatorics and cryptography are interacted significantly. In this talk, I will present several concrete examples to illustrate how combinatorial objects and techniques are applied to the constructions of cryptographic schemes such as in secret sharing, threshold cryptography and secure multiparty computation. |
| 专家简介 | Huaxiong Wang received a PhD in Mathematics from University of Haifa, Israel in 1996 and a PhD in Computer Science from University of Wollongong, Australia in 2001. He has been with Nanyang Technological University (NTU) in Singapore since 2006, where he also served as the Head of Division of Mathematical Sciences from 2013 to 2015. He is currently the Co-Director for The National Centre for Research in Digital Trust (NCTD) and the Deputy Director of Strategic Centre for Research in Privacy-Preserving Technologies & Systems (SCRIPTS) at NTU. He has more than 25 years of experience in cryptography and information security. He is author/co-author of 1 book, 9 edited books and over 250 papers in international journals and conferences, covering various areas in cryptography and information security. He has supervised over 30 PhD students, and has served on the editorial board of several international journals and as a member/chair of the program committee for more than 100 international conferences. He received the inaugural Award of Best Research Contribution awarded by the Computer Science Association of Australasia in 2004. He was the program Co-Chair of Asiacrypt 2020 and 2021. |

| | |
|---|---|
| 报告专家 | Lein Harn（美国密苏里大学） |
| 报告题目 | My Recent Research on Secret Sharing, Key Distribution and Group Authentication |
| 报告摘要 | I have published the first group authentication paper in IEEE Trans. on Computers in 2013. Since then, there are many publications related to this subject. In group authentication, group members obtain tokens from a dealer and the dealer generates tokens based on Shamir's (t, n) threshold secret sharing scheme. In this talk, first, I will introduce my recent research on the threshold scheme. Then, I will address how to apply these modifications of threshold scheme to various security problems and solutions on group authentication, data collection, secure multiparty computations. Finally, I will introduce an extremely lightweight key distribution with authentication. In summary, I will only present high-level concepts without giving any detail discussion. |
| 专家简介 | Lein Harn received the B.S. degree in electrical engineering from the National Taiwan University in 1977, the M.S. degree in electrical engineering from the State University of New York-Stony Brook in 1980, and the Ph.D. degree in electrical engineering from the University of Minnesota in 1984. He has been a Professor at the Department of Electrical and Computer Engineering, University of Missouri- Kansas City (UMKC), USA, since 1984. He has retired from UMKC since 2019. |

| | |
|---|---|
| 报告专家 | 赖俊祚（暨南大学） |
| 报告题目 | 选择打开安全的公钥加密 |
| 报告摘要 | 公钥加密的传统安全模型 IND-CPA/CCA 只考虑了一个用户的情况。而实际部署的公钥加密是在多用户环境中的。在多用户环境中，敌手可能渗透某些用户获取其内部信息，如发送或接收的消息、加密用的随机数或解密密钥。已有研究结果表明：传统 IND-CPA/CCA 安全的公钥加密在上述的敌手攻击环境下无法提供相应的安全保障。Bellare 等人在 EUROCRYPT'09 上提出选择打开安全公钥加密的概念，保障在上述敌手攻击下未被渗透用户信息的安全性。报告介绍了选择打开安全公钥加密的概念和现状以及我们的相关工作。 |
| 专家简介 | 赖俊祚，暨南大学信息科学技术/网络空间安全学院研究员，博士生导师。研究方向为密码学与信息安全，研究成果发表在 EUROCRYPT、ASIACRYPT、PKC、ACM TISSEC、IEEE TIFS、IEEE TDSC、DCC 等密码学和信息安全国际会议和国际期刊上。担任中国密码学会区块链专委会委员和青工委委员，广东省计算机学会区块链专委会副主任委员和青工委常务委员等。主持国家自然科学基金优秀青年项目、广东省卓越青年团队项目、广东省自然科学基金杰出青年项目等项目。 |

| | |
|---|---|
| 报告专家 | Vladimir Edemskiy（俄罗斯诺夫哥罗德国立大学） |
| 报告题目 | The 4-adic complexity of generalized cyclotomic quaternary sequences with a period of $2p^m$ |
| 报告摘要 | The $m$-adic complexity is an important characteristic of pseudorandom sequences. It is defined as the shortest length of a feedback with carry shift register<br>that can generate this sequence. Quite a lot is known about 2-adic complexity of binary sequences. Unlike binary sequences, it seems that the study of the 4-adic complexity of quaternary sequences has not been fully developed.<br>In this talk, we generalize the results about the 4-adic complexity of series of sequences of length $2p$ obtained earlier and study of the 4-adic complexity of generalized quaternary cyclotomic sequences with period $2p^n$ where $p$ is a prime. Sequences are defined using classes of quadratic and biquadratic residues modulo $2p^n$. The definitions of these sequences were proposed by Ke et al. They have high linear complexity over the finite field of order four and finite ring of order four.<br>We obtain the estimates of the 4-adic complexity of a few families of quaternary sequences. Our results show that the 4-adic complexity of these sequences is large enough to effectively resist the attacks of the of the rational approximation algorithm. |
| 专家简介 | Vladimir Edemskiy was born in 1958. He graduated from Leningrad University with a degree in Mathematics and completed the post-graduate course in this university. He received the Ph.D. degree in Algebra and Number Theory from Leningrad University. In 2010, he received the D. Sc. degree from Novgorod State University. Now he is a professor of the Department of Applied Mathematics and Information Science, Yaroslav-the-Wise Novgorod State University.<br>Vladimir Edemskiy lectures to bachelors, masters and postgraduates. His research interests include pseudorandom sequences, design sequences and cryptography. He was the leader of several scientific research projects devoted to the study of the properties of sequences. In particular, Professor Zhixiong Chen and Vladimir Edemskiy together fulfilled a Russian – Chinese grant in 2019-2020. He is a reviewer of IEEE Transactions on Information Theory, Designs, Codes and Cryptography, Cryptography and Communications-CCDS, Advances in Mathematics of Communications and other international journals. |

| 报告专家 | 施敏加（安徽大学） |
| --- | --- |
| 报告题目 | Equivalence and Duality of Polycyclic Codes Associated with Trinomials over Finite Fields |
| 报告摘要 | In this talk, all of the conjectures in [Nuh Aydin, Peihan Liu, Bryan Yoshino: Polycyclic Codes Associated with Trinomials: Good Codes and Open Questions, Designs, Codes and Cryptography, 90(5): 1241-1269 (2022).] are settled: some proven correct, some proven correct with a modification, and some disproven, involving the equivalence and duality of polycyclic codes associated with trinomials. We also give methods to construct isodual and self-dual polycyclic codes, and study the self-orthogonal and dual-containing polycyclic codes over $\mathbb{F}_2$. |
| 专家简介 | 施敏加，安徽大学数学科学学院副院长，教授，博士生导师。先后入选安徽省杰出青年基金支持计划，安徽省学术与技术带头人和 2019 年高校学科（专业）拔尖人才计划和 2020 年全球前 2%顶尖“年度影响力”科学家榜单。先后荣获第二届“安徽省青年数学奖”、安徽省自然科学一等奖和安徽省自然科学二等奖各一项，并获教育部宝钢优秀教师奖和安徽省教学成果奖一等奖。主持国家自然科学基金 4 项，安徽省自然科学基金杰出青年基金等省部级重点项目多项。应邀以主编身份在 Elsevier 出版社和 World Scientific 出版社出版英文学术专著 2 部，在 IEEE TIT, DCC, FFTA 等国内外权威学术期刊上发表期刊论文 100 余篇，研究成果入选《世界简明编码理论百科全书》，多篇论文入选 ESI 高被引论文。曾应邀访问新加坡、法国、俄罗斯、韩国等多个国家。 |

| 报告专家 | Chulei Li（挪威卑尔根大学） |
| --- | --- |
| 报告题目 | On decoding of rank-metric codes |
| 报告摘要 | Since introduced by Delsarte and Gabidulin, rank-metric codes have found applications in random networking, criss-cross error correction, distributed storage and cryptography. Existing researches on the topic have mainly focused on bound analysis, construction and efficient decoding of rank-metric codes. In recent years, several interesting types of rank-metric codes, such as new maximum-rank distance codes, optimal matrix codes, low-rank parity-check codes, were proposed and some found applications in post-quantum cryptography. On the other hand, the study of efficient decoding of rank-metric codes somewhat falls behind. In this talk, I will review our recent work on decoding of rank-metric codes. |
| 专家简介 | Chunlei Li received the Ph.D. degree from the University of Bergen, Norway in 2014. He was a postdoc at the University of Stavanger, Norway, during 2015-2017, and a researcher at the University of Bergen during 2017-2018. Since 2018, he has been an associate professor with the Department of Informatics, University of Bergen. His research interests include sequence design, coding theory and cryptography. He was the program co-chairman of the workshop Sequences and Their Applications (SETA20), 2020 and a TPC member of the workshops WAIFI19, SETA18, IWSDA19/22, BFA20/21/22, WCC2022 and ITW2023. |

| 报告专家 | 夏永波（中南民族大学） |
| --- | --- |
| 报告题目 | More Properties about A Family of Ternary Almost Perfect Nonlinear Mappings |
| 报告摘要 | Let $n$ be an odd integer, $d_1=\frac{3^n-1}{2}-1$, $d_2=3^n-2$, and $f_u(x)=ux^{d_1}+x^{d_2}$ be a mapping from $\mathbb{F}_{3^n}$ to itself, where $u\in\mathbb{F}_{3^n}$. In this talk, we show that $f_u(x)$ is an almost perfect nonlinear(APN) mapping from $\mathbb{F}_{3^n}$ to $\mathbb{F}_{3^n}$ if and only if $\mathcal{X}(u+1)=\mathcal{X}(u-1)=\mathcal{X}(u)$, where $\mathcal{X}(\bullet)$ denotes the quadratic character of $\mathbb{F}_{3^n}$. This settles the open problem raised by Ness and Helleseth in 2007. In addition, the differential properties of $f_u(x)$ are further investigated. Especially, for some $u$ in $\mathbb{F}_{3^n}$, the differential spectrum of $f_u(x)$ is completely determined. Our results can also be generalized to the case $p\equiv 3(\mathrm{mod}\,4)$. |
| 专家简介 | 夏永波，男，教授，硕士生导师。2009 年 6 月毕业于湖北大学数学系，获理学博士学位；2013 年 9 月至 2014 年 9 月，受留学基金委资助，赴挪威卑尔根大学访学，合作导师为 IEEE Fellow、挪威科学院院士 Tor Helleseth 教授。目前的研究兴趣为：无线通信中的序列设计、编码和密码学；讲授的主要课程有：数学分析（本科），高等数学（本科），线性代数（本科），代数学引论（研究生），编码理论导论（研究生）等。主持国家自然科学基金项目 3 项（面上 2 项，青年 1 项），湖北省自然科学基金 2 项，科技部外专项目 2 项，国家民委高等教育教学改革研究项目 1 项；在《IEEE Transactions on Information Theory》、《Finite Fields and Their Applications》、《Cryptography and Communications》、《Science China Mathematics》等期刊上发表论文 30 余篇。曾获 2018 年湖北省自然科学奖二等奖（排名 2）、2019 年国家民委教学成果二等奖（排名 1）、2018 年湖北省教学成果奖三等奖（排名 3），2019 年入选国家民委青年教学标兵，2020 年入选国家民委中青年英才。 |

| 报告专家 | 常祖领（郑州大学） |
| --- | --- |
| 报告题目 | *k*-置换广义圈的计数与构造<br>（Enumerations and Constructions of Universal Cycles for *k*-permutations） |
| 报告摘要 | *k*-置换即为 *n* 元置换的 *k* 长部分，而 *k*-置换广义圈是一个 *n* 元周期序列满足每个 *k*-置换均作为其中的 *k* 元组且仅出现一次。*k*-置换广义圈是著名的 de Bruijn 序列(又称 M-序列)的一种推广。*k*-置换广义圈的计数问题一直没有得到解决，而快速生成 *k*-置换广义圈具有重要的应用价值。本报告将介绍该问题的一些研究进展，给出了一种新的计数方法，并给出 *k* 比较小时的精确计数公式。本报告还将给出一种快速生成(*n*-1)-置换广义圈的方法，具有空间复杂度 *O*(*n*)和时间复杂度 *O*(1)。 |
| 专家简介 | 常祖领，郑州大学数学与统计学院，教授，博士生导师，副院长。主要研究方向是序列设计与分析，在 M-序列研究方面有系列成果。现已主持国家自然科学基金 3 项，省级项目多项。 |

| | |
|---|---|
| 报告专家 | 程航（福州大学） |
| 报告题目 | 基于外包加密监控视频的安全可验证行人再识别技术 |
| 报告摘要 | 行人再识别由于其能够鉴别来自不同监控视频中感兴趣的人而引起了广泛关注。随着监控视频数量的增加，高计算和存储成本给资源受限的用户带来了巨大的挑战。近年来，云存储服务使得大规模的视频数据外包成为可能。然而，对外包监控视频的行人重新识别可能会导致安全威胁，即可能会导致这些视频中相关行人的隐私泄露。针对外包监控视频的行人重识别可能会导致安全威胁，我们提出了一个高效的隐私保护行人重识别方案。 |
| 专家简介 | 程航，福州大学教授、博士、博士生导师，福州大学数学与统计学院副院长。研究方向包括：多媒体安全、图像处理、加密算法、信息隐藏等。近年来，在 IEEE TDSC、IEEE TCSVT、IEEE SPL、Information Sciences 等国内外期刊上发表学术论文 30 余篇，Google 引用 500 余次；先后主持 1 项国家自然科学基金面上项目，2 项福建省自然科学基金面上项目，参与 5 项国家自然科学基金项目，申请国家发明专利 10 余项（已授权 5 项）；主持和参与省校级教改项目 10 余项，发表教改论文 10 余篇，指导学生获得 1 项美国大学生数学建模竞赛特等奖（同时又获冠名奖）；担任中国数字媒体取证与安全专委会委员，中国工业与应用数学学会会员；担任 IEEE TDSC、IEEE TII、IEEE TCC、Information Sciences 等 20 余个国内外重要期刊审稿人。 |

| | |
|---|---|
| 报告专家 | 祝辉林（厦门大学） |
| 报告题目 | Some Time-Asymmetric Encoding Schemes Based on *N*-th Root and Discrete Logarithm Problem over a Finite Field |
| 报告摘要 | A verifiable delay function (VDF) is a function that requires a specified number of sequential steps of computation whose correctness can be efficiently and publicly verified. Verifiable delay encoding (VDE) is a kind of pseudo-VDF with efficient decoding. It is an important part of the construction of replication proof in Filecoin which is a decentralized storage network designed to store humanity's most important information. The VDE used in Filecoin is Sloth algorithm. We study and improve Sloth algorithm and Sloth++ algorithm on its extended domain and provide a new scheme based on discrete logarithm problem. This is a joint work with Luo and You. |
| 专家简介 | 祝辉林，厦门大学数学科学学院副教授、硕士生导师，武汉大学博士，山东大学博士后，加拿大英属哥伦比亚大学访问学者。主要从事数论与密码学的研究，特别是丢番图方程、计算数论和密码学算法分析设计及实现等。曾主持国家自然科学基金、福建省自然科学基金和中央高校基本科研业务费专项资金等科研项目多项。目前，已经在《Acta Arithmetica》、《Journal of Number Theory》、《Quarterly Journal of the Mathematics》等期刊发表论文 20 余篇。 |

# 学院简介

百载春秋，薪火相传。学院肇始于1907年创办的“福建优级师范学堂”的数学科。后由华南女子文理学院、福建协和大学、福建省立师范专科学校等院校几经调整合并，于1953年成立福建师范学院，保留发展了数学系。1972年，改名为福建师范大学数学系。1996年，成立计算机科学系，与数学系合称为福建师范大学数学系、计算机科学系。2002年，成立数学与计算机科学学院、软件学院。2017年6月，数学与计算机科学学院、软件学院整合成立数学与信息学院。2021年6月，数学与信息学院分设数学与统计学院、计算机与网络空间安全学院（软件学院）。

学院现设数学系、统计学系和实验教学中心，拥有数学与应用数学（师范类）、统计学2个本科专业。数学与应用数学专业是国家级特色专业、入选国家级一流本科专业建设点，通过教育部师范类专业二级认证。学院获得国家级教学成果二等奖1项、福建省第七届优秀教学成果一等奖1项；获批本科质量工程国家级项目4项、省级7项；获得国家级一流课程1门、省级一流课程3门；省级人才培养模式创新实验区1个、省级研究生教育创新基地1个；获得省优秀博士论文1篇。学生在国际数学建模竞赛、全国大学生数学建模竞赛、全国研究生数学建模、全国大学生数学竞赛等赛事上屡获佳绩。

现有数学、统计学2个一级学科博士学位授权点，数学、统计学2个博士后科研流动站，数学、统计学2个一级学科硕士学位授权点。现有学科教学（数学）、应用统计2个专业学位硕士点。数学是福建省高峰学

科，统计学是福建省重点学科。现有福建省分析数学及应用重点实验室、福建省应用数学中心和福建师范大学数学研究中心、福建数学基础教育研究中心等科研平台。学院主办《福建中学数学》杂志。学院是福建省中小学数学学科教学带头人培养基地。

学院高度重视高层次人才队伍建设，师资力量雄厚。现有在职教职工102人，其中教授28人、副教授36人；博士研究生导师16人；国家杰出青年基金2人，国家优秀青年基金1人；国务院政府特殊津贴1人；长江学者1人，闽江学者7人；德国洪堡基金1人；入选福建省“百人计划”2人、福建省“百千万人才工程”3人、福建省优秀教师1人、福建省“运盛”青年科技奖1人。学院获得教育部自然科学奖一等奖1项，教育部科技进步奖二等奖1项，交通部科技进步奖二等奖1项；福建省科技进步奖二等奖6项；福建省科学技术奖二等奖2项、三等奖4项；福建省社会科学奖二等奖1项、三等奖1项。

学院已为党和国家培养了许多优秀的人才，他们积极工作，奋发向上，成为各行业的骨干，为教育发展、经济建设和社会进步做出了重要的贡献。李迅、江文哉、张远南、王毓泉、叶青柏、刘金星、李必成、林风、林琳、林群、林燎、林顺来、郑一平、邵东生、周灵、徐明杰等校友荣获“福建省杰出人民教师”荣誉称号。广大校友爱国爱校，慷慨解囊，捐资助学。2006年，福建师范大学数学系61级学生、香港知名企业家、福建师范大学客座教授吴维新先生捐资设立“吴维新教育基金”，2015年，吴维新先生再次捐资设立“吴维新研究生奖学金”。