信息编码理论与应用研讨会

程序册

2026 年 6 月 27 日

西安电子科技大学广州研究院

西安电子科技大学 XIDIAN UNIVERSITY | 广州研究院 Guangzhou Institute of Technology

目　录

会议信息

1. 会议简介

为推动国家重点研发计划项目“面向未来无线通信信息处理若干关键问题的数学理论和方法”的研究，促进国内编码与信息论相关领域的发展，将于 2026 年 06 月 27 日在广州举办“信息编码理论与应用研讨会”。本次论坛由西安电子科技大学广州研究院主办，中国电子学会信息论分会协办，诚邀广大专家学者拨冗参会！

2. 会议日期和地点

日期：2026 年 6 月 27 日

地点：西安电子科技大学广州研究院 · 求真楼三楼 · 无限畅想室

位置：广东省广州市黄埔区中新广州知识城知明路 83 号 （参见下页俯瞰图）

3. 会务联系人

陈超：cchen@xidian.edu.cn；15091890020

刘凌：liuling@xidian.edu.cn;　13823387621

曹琦：caoqi@xidian.edu.cn;　16676721110

4. 附近酒店

1. 专家美居(西安电子科技大学广州研究院店)见下页俯瞰图，离会议地点约 100 米

2. 广州知识城 MUSTEL 木文缇酒店　距离会议地点约 3 公里

3. 开芯国际大酒店　距离会议地点约 4 公里

广州研究院楼宇俯瞰图

会议议程

日期	时间	事项	报告人
06月27日	8:30-8:40	**会议签到**	所有参会人员
	8:40-8:50	**会议致辞**	
	8:50-9:30	**Linear Recurring Sequences, Subfield Subcodes and Trace Codes of Cyclic Codes**	符方伟 南开大学
	9:30-10:10	**New Bounds for Binary Linear Codes via the Weight Hierarchy**	马啸 中山大学
	10:10 -10:30	**茶歇**	
	10:30-11:10	**Secure Network Function Computation**	光炫 南开大学
	11:10-11:50	**Polynomial Commitments for Galois Rings and Applications to SNARKs over $\mathbb{Z}_{2^k}$**	李宋宋 上海交通大学
	12:00-14:30	**午餐**	
06月27日	14:30-15:10	**MIMO 信号检测问题研究的发展与挑战**	王正 东南大学
	15:10-15:50	**Algebraic Constructions of Block MDS LDPC Codes**	朱宏伟 广州大学
	15:50-16:10	**茶歇**	
	16:10-16:50	**基于信息瓶颈理论的语义信息处理和传输**	吴幼龙 上海科技大学
	16:50-17:30	**Foundation of Multichannel Prefix Codes**	Hoover Ho Fai Yin 香港中文大学
	17:30-17:50	**On the Capacity of Single-Label DNA Labeling**	邬子涵 西安电子科技大学
	18:00	**晚餐**	

报告简介

报告一：Linear Recurring Sequences, Subfield Subcodes and Trace Codes of Cyclic Codes

➢ **报告人：**符方伟 教授 南开大学

➢ **报告摘要：**

Linear recurring sequences have important applications in cryptography and coding theory. We introduce and present some important relationship among linear recurring sequences, subfield subcodes and trace codes of cyclic codes.

➢ **报告人简介：**

符方伟，分别于 1984 年、1987 年和 1990 年获得南开大学理学（数学）学士、硕士和博士学位。1987 年 7 月至今在南开大学工作。现为南开大学陈省身数学研究所教授和博士生导师、中国工业与应用数学学会编码密码及相关组合理论专业委员会副主任委员、中国电子学会信息论分会副主任委员、中国密码学会密码数学理论专委会顾问和委员、学术期刊《密码学报》的编委。入选 2000 年度教育部跨世纪优秀人才培养计划。2000 年获国务院政府特殊津贴。曾经担任中国工业与应用数学学会第八届理事会理事、中国密码学会第一届至第四届理事会理事、中国密码学会密码数学理论专委会第一届至第三届副主任委员、学术期刊《应用数学》第三届编委会的编委和《电子与信息学报》的编委。主要从事编码理论及其应用、密码学及其应用、信息论及其应用的研究工作，在国际和国内重要学术期刊与国际会议论文集上发表论文 300 余篇。作为负责人承担了国家自然科学基金和教育部的多项科研项目，作为课题负责人承担了科技部 973 项目和国家重点研发计划项目。

报告二：New Bounds for Binary Linear Codes via the Weight Hierarchy

➢ 报告人：马啸 教授 中山大学

➢ 报告摘要：

The well-known Singleton bound states that a binary linear block code $C[n,k,d]$ of length n,dimension k,and minimum distance d must satisfy $k \le n-d+1$ which, in the case of $n>d>4$, can be tightened by the Ma--Wang bound, stating that $k \le n-d+1-\lceil \log_2(n-d+1) \rceil$.In this paper, the Ma--Wang bound is further generalized and hence tightened in the case of $n>d>8$.The key is to apply the Hamming bound, also known as the sphere-packing bound, to a properly constructed residual code.Specifically, puncturing C on the support of a minimum-weight codeword produces a residual code with parameters $[n-d, k-1, \ge \lceil d/2 \rceil]$, which implies $k \le n-d+1-\left\lceil \log_2 \sum_{i=0}^{\lfloor (d-1)/4 \rfloor} \binom{n-d}{i} \right\rceil$. The same procedure can be extended by invoking the weight hierarchy of the code as follows.Let $U_r \le C$ be a subcode that attains the $r-th$ generalized Hamming weight $d_r(C)$ .Then puncturing C on (U_r) produces a residual code with parameters $[n-d_r(\mathrm{C}), k-r, \ge d_{r+1}(\mathrm{C})-d_r(\mathrm{C})]$,which, by the Hamming bound, implies $k \le n-d_r(\mathrm{C})+r-\left\lceil \log_2 \sum_{i=0}^{\left\lfloor \frac{d_{r+1}(\mathrm{C})-d_r(\mathrm{C})-1}{2} \right\rfloor} \binom{n-d_r(\mathrm{C})}{i} \right\rceil$. Since the weight hierarchy is usually unknown, we further derive upper bounds depending only on (n,d) by replacing the unknown weight-hierarchy terms with their bounds.Numerical comparisons with several well-known bounds show that the proposed bounds can be tighter in certain parameter regimes.The same argument can also be adapted to nonbinary linear block codes.

➢ 报告人简介：

Xiao Ma received the Ph.D. degree in communication and information systems from Xidian University, China in 2000. He is a Professor at the School of Computer Science and Engineering, Sun Yat-sen University, Guangzhou, China. From 2000 to 2002, he was a Post-Doctoral Fellow with Harvard University, Cambridge. MA, USA. From 2002 to 2004, he was a Research Fellow with the City University of Hong Kong. His research interests include information theory, channel coding theory and decoding algorithms.

报告三：Secure Network Function Computation

➢ 报告人：光炫 教授 南开大学

➢ 报告摘要:

该报告将介绍安全网络函数计算问题以及近来的研究进展。安全网络函数计算研究如何在通信网络上安全地计算目标函数，其核心问题是安全网络函数计算容量的刻画，包括容量界和码构造。然而，对于安全网络函数计算的一般性模型，该容量的刻画是极其困难。本报告的研究工作聚焦于线性目标函数，针对两类典型的安全要求，即安全函数为恒等函数和线性目标函数（信源消息安全和目标函数安全），给出了容量的普适上界（适用于任何网络拓扑和安全级别）、上界的高效计算方法以及码构造方案；并完全刻画了多类模型的容量。

➢ 报告人简介：

光炫，南开大学教授、博导，数学学科学术委员会委员、数学科学学院副院长、教育部“核心数学与组合数学”重点实验室固定研究人员。入选国家青年人才项目、香江学者计划和南开大学百名青年学科带头人培养计划。2012 年毕业于南开大学陈省身数学研究所，获博士学位，曾在美国南加州大学及香港中文大学从事研究工作近 5 年。研究兴趣为信息论、编码理论与密码学；目前的研究方向为面向函数计算的信息论和编码。近年来出版一部学术专著（一作），由德国 Springer 出版；发表学术论文 60 余篇，其中在信息论、安全和通信理论的权威期刊和会议上发表论文 30 余篇，包括 IEEE Trans. Inf. Theory, IEEE J. Sel. Areas Inf. Theory, IEEE J. Sel. Areas Commun., IEEE Trans. Inf. Foren. Sec., USENIX Security,《中国科学》等，研究成果获多个国内外会议的最佳论文奖。曾获天津数学与统计“青年学者奖”，中国电子学会“信息论青年新星奖”，“香江学者奖”等。主持重点研发计划课题、基础加强重点研究课题、基金委国际合作研究项目等省部级基金项目多项以及企业科技项目，获田家炳教育基金资助。

报告四： Polynomial Commitments for Galois Rings and Applications to SNARKs over $\mathbb{Z}_{2^k}$

➢ 报告人：李宋宋 助理研究员 上海交通大学

➢ 报告摘要：

Succinct non-interactive arguments of knowledge (SNARKs) allow a weak verifier to delegate computation tasks to a powerful prover in a verifiable way. However, most SNARK constructions require the computation tasks to be represented as arithmetic circuits over finite fields, incurring a significant overhead when applied for delegations of modern computer programs, which typically are of $Z_{2^{64}}$ or $Z_{2^{64}}$ arithmetic.

Towards building publicly verifiable SNARKs for rings Z_{2^k} we follow the well-established framework of polynomial interactive oracle proofs (IOP)-based SNARKs, and obtain the following results:

i) We systematically study the proximity gaps for Reed-Solomon codes over Galois rings. We prove that for Galois rings, the state-of-the-art $(1-\rho)/2$ gap for finite fields given by Ben-Sasson et al. (JACM 2023) still holds. This allows to construct efficient polynomial commitment schemes for Galois rings based on Reed-Solomon codes.

ii) We construct efficient polynomial IOPs for rank one constraint systems (R1CS) over Z_{2^k} via Galois rings. To amortize the overhead of operating on a large Galois ring extension of Z_{2^k}, we make use of the reverse-multiplication friendly embeddings (RMFEs) techniques.

iii) Combining the above two ingredients together, we put forward the first publicly verifiable SNARKs for rings Z_{2^k} with a transparent setup and plausibly post-quantum security. In addition, we implement and evaluate our constructions. Our evaluations indicate the concrete efficiency is promising, provided that Galois rings operations are optimized well.

➢ 报告人简介 ：

李宋宋博士，目前为上海交通大学计算机学院助理研究员。2020 年获得中国科学技术大学数学专业博士学位。2020 年-2022 年在上海交通大学从事博士后研究工作。研究领域包括代数编码及其在密码学中的应用、椭圆曲线密码等。

报告五：MIMO 信号检测问题研究的发展与挑战

➢ 报告人：王正 副教授 东南大学

➢ 报告摘要：

MIMO 信号检测是无线通信接收机设计中的核心问题，其目标是在有限计算复杂度下实现对多天线传输信号的可靠恢复。随着无线通信系统从传统 MIMO 发展到大规模 MIMO，再到超大规模 MIMO，系统维度、信道结构和应用场景均发生了显著变化，传统检测算法在计算复杂度、收敛性能和硬件实现方面面临新的挑战。本报告将围绕 MIMO 信号检测问题的基本模型、典型算法和发展脉络展开介绍，并进一步讨论在超大规模天线、近场传播、信道非平稳性和通算智融合背景下 MIMO 信号检测研究所面临的关键问题与发展机遇。

➢ 报告人简介：

王正，东南大学副教授、博士生导师、江苏省双创博士、IEEE 高级会员，连续入选爱思唯尔 2023、2024 年度信息与通信工程学科“中国高被引学者”。近年来，主持包含国家自然科学基金重点项目子课题，面上项目，青年项目等十多项基金项目，发表研究论文成果 80 余篇，包括国际权威期刊 IEEE TIT、TSP、TWC、TCOM 等，荣获 2026 年 IEEE ICC Best Paper Award，2024 年江苏省科技进步奖一等奖，2023 年华为技术有限公司“火花奖”等，担任 Chinese Journal of Electronics (CJE)等期刊的青年编委以及 VTC、ICMLCN、IWCMC 等国际会议的联席主席。

报告六：Algebraic Constructions of Block MDS LDPC Codes

➢ **报告人：**朱宏伟 讲师 广州大学

➢ **报告摘要：**

Array code construction is a key algebraic technique for designing low-density parity-check (LDPC) codes. Block maximum distance separable (MDS) LDPC codes refer to a special class of LDPC codes whose parity-check matrices fully match those of MDS array codes, and they have been successfully applied in high-dimensional quantum key distribution (QKD) systems. A review of existing studies shows that there is currently no explicit construction method for infinite families of binary and non-binary block MDS LDPC codes, with only several isolated non-binary code examples available in the literature, which constitutes an unaddressed research gap. Targeting this gap, this report integrates MDS array codes with algebraically constructed LDPC codes and proposes four optimized dispersion construction rules. In particular, this work develops an innovative matrix dispersion framework named the Punctured Circulant Permutation Matrices-Dispersion-Superposition (PUCPM-D-SP) construction. With Vandermonde matrices as the base matrices and under reasonable algebraic constraints, we construct an infinite family of binary block MDS LDPC codes using the PUCPM-D-SP method. Theoretical analysis further verifies that linear codes derived from the parity-check matrix of Blaum-Roth codes are binary block MDS LDPC codes with no 4-cycles. In addition, when adopting Moore matrices as base matrices, the proposed construction can generate a family of nearly optimal binary MDS LDPC codes, and the parity-check matrix of each code in this family is the Boolean complement of the parity-check matrix of an MDS array code.

➢ **报告人简介：**

朱宏伟，博士，广州大学特聘讲师。2023 年博士毕业于安徽大学，博士导师为施敏加教授。2023-2025 年于清华大学深圳国际研究生院从事博士后研究，合作导师为夏树涛教授。主要从事编码理论与密码学研究。发表 SCI 期刊发表论文 20 篇，其中 IEEE TIT 5 篇。主持博士后面上项目两项，广东省粤穗联合基金一项。

报告七：基于信息瓶颈理论的语义信息处理和传输

➢ 报告人：吴幼龙 副教授 上海科技大学

➢ 报告摘要：

未来通信将以人为核心、以目标为导向来构建“智慧内生”网络。语义通信作为新的通信范式，仅关注传输与任务相关的语义信息，因此能显著降低通信开销和提升用户体验。现有语义通信方案通常采用深度学习算法对特定任务场景进行单独设计，面临着可解释性差、可扩展性低以及缺乏统一理论指导等挑战。本报告将以香农率失真和联合信源信道编码理论为指导，拓展信息瓶颈理论在语义通信的应用，提出面向多任务语义通信的多重率失真理论，构建鲁棒高效、隐私安全的联合信道信道语义编码框架，旨在提出统一且有效的理论原则来指导语义信息处理和传输，解决语义通信的任务多目标、信道噪声干扰等问题，实现高效、可解释、可拓展的语义通信。

➢ 报告人简介：

吴幼龙博士现任上海科技大学常任副教授、研究员、博导。研究方向主要包括网络信息论、语义通信和边缘人工智能。吴博士本科毕业于武汉大学电子工程系，硕士毕业于上海交通大学信息工程系，博士毕业于巴黎高科高等电信学院。2014～2016 年，他加入慕尼黑工大从事博士后和高级研究员工作。目前已在 IEEE TIT、JSAC、TON、TIFS、TCOM 等国际重要期刊及会议上发表学术论文 80 余篇，主持国家自然科学基金面上项目、国家自然科学基金青年项目、上海市科委/教委等支持的多个项目。吴博士于 2017 年获得德国洪堡学者荣誉，2018 年入选上海浦江人才计划，2024 年入选上海市通信学会青年英才。

报告八：Foundation of Multichannel Prefix Codes

➢ 报告人：Hoover Ho Fai Yin 讲师 香港中文大学

➢ 报告摘要：

A natural generalization of the classical theory of prefix codes is to extend from single channel to multiple channels. In a multichannel prefix code, every codeword is a tuple, where each component is associated with a channel. Not all classical results can be generalized directly due to the increase of dimensions. In this talk, we focus on two topics that cannot be generalized directly: 1) Constructing 2-channel prefix codes from a given set of codeword lengths; and 2) Existence of optimal tree-decodable codes that are not optimal prefix codes.

➢ 报告人简介：

Dr. Yin is a Lecturer at the Department of Information Engineering, The Chinese University of Hong Kong. He received his Ph.D. in Information Engineering from The Chinese University of Hong Kong in 2019. His research interest mainly lies in the field of network coding. Besides that, he is also interested in computer and network systems, information hiding and steganography, source coding, and recreational mathematics.

报告九：On the Capacity of Single-Label DNA Labeling

➢ **报告人：**邬子涵 硕士研究生 西安电子科技大学

➢ **报告摘要：**

This report studies the DNA labeling problem and shows that the labeling capacity can be formulated as a zero-error capacity problem. In the single-label setting, each case can be modeled as a star graph, for which we construct a zero-error coding scheme and prove its rate optimality. This fully characterizes the labeling capacity in the single-label setting, which is equivalent to determining the zero-error capacity of star graphs.

➢ **报告人简介：**

Zihan Wu is currently a master's student at the Guangzhou Institute of Technology, Xidian University. Her research focuses on zero-error information theory, with recent work on DNA labeling capacity and the zero-error capacity characterization of broadcast channels. She has published two related papers.