编码密码中的数学理论

Mathematical theories in coding and cryptography

会议手册

中国•云南

2026 年 7 月 12 日-18 日

目录

会议报到时间：2026 年 7 月 12 日

会议报到地点：昆明天元数学国际交流中心

会议时间：2026 年 7 月 12 日至 18 日

会议地点：昆明天元数学国际交流中心

会议召集人：

陈　豪（暨南大学）

周海燕（南京师范大学）

张　俊（首都师范大学）

会 议 日 程

日期	时间	会议内容	主持人
7 月 13 日 星期一	8:50-9:00	**开幕式**	
	9:00-10:00	**报告题目：**Sol 3-流形的手征性与实二次算术 **报告人：**田野 中国科学院数学与系统科学研究院	
	10:00-10:30	**讨论**	
	10:30-11:30	**报告题目：**Post-quantum Cryptography, A New Era **报告人：**丁津泰 西交利物浦大学	
	11:30-14:30	**午餐**	
	14:30-15:30	**报告题目：**MDS Array Codes: Theoretical Bounds and Practical Constructions **报告人：**胡思煌 山东大学	
	15:30-16:00	**讨论**	
	16:00-18:00	**专题讨论：**经典与量子纠错码构造及其相关数论组合问题	
	18:00	**晚餐**	

日期	时间	会议内容	主持人
7 月 14 日 星期二	9:00-10:00	**报告题目：**On permutation polynomials of index q+1 over $\mathbb{F}_{q^2}$ **报告人：**王强 Carleton University	
	10:00-10:30	**讨论**	
	10:30-11:30	**报告题目：**The automorphism groups of random linear codes **报告人：**王琦 南方科技大学	
	11:30-14:30	**午餐**	
	14:30-15:30	**报告题目：**Further results on bent partitions **报告人：**王佳鑫 合肥工业大学	
	15:30-16:00	**讨论**	
	16:00-18:00	**专题讨论：**序列与密码函数	
	18:00	**晚餐**	

会 议 日 程

日期	时间	会议内容	主持人
7 月 15 日 星期三	9:00-10:00	**报告题目：** Several famous conjectures related to polynomials representing primes **报告人：**秦厚荣 南京大学	
	10:00-10:30	**讨论**	
	10:30-11:30	**报告题目：** A Structural Characterization of Cyclotomic Cosets with Applications to Affine-Invariant Codes and BCH Codes **报告人：**郑大彬 湖北大学	
	11:30-14:30	**午餐**	
	14:30-15:30	**报告题目：** On the Niho type locally-APN power functions and their boomerang spectrum **报告人：**李念 湖北大学	
	15:30-16:00	**讨论**	
	16:00-18:00	**专题讨论：**编码中困难问题及其在后量子密码中的应用	
	18:00	**晚餐**	

日期	时间	会议内容	主持人
7 月 16 日 星期四	9:00-10:00	**报告题目：**唯一可译的网络函数计算编码 **报告人：**光炫 南开大学	
	10:00-10:30	**讨论**	
	10:30-11:30	**报告题目：**Good families of binary sequences with low correlation and high linear complexity via function fields **报告人：**马立明 中国科学技术大学	
	11:30-14:30	**午餐**	
	14:30-18:00	**自由活动**	
	18:00	**晚餐**	

会 议 日 程

日期	时间	会议内容	主持人
7 月 17 日 星期五	9:00-10:00	**报告题目：**基于同源的后量子密码体系 **报告人：**欧阳毅 中国科学技术大学	
	10:00-10:30	**讨论**	
	10:30-11:30	**报告题目：**Locally Repairable Codes with Availability via Elliptic Function Fields **报告人：**赵昌安 中山大学	
	11:30-14:30	**午餐**	
	14:30-15:30	**报告题目：**A Novel Leakage Model in OpenSSL's Miller-Rabin Primality Test **报告人：**胡红钢 中国科学技术大学	
	15:30-16:00	**讨论**	
	16:00-18:00	**专题讨论：**格与同源问题及其在后量子密码中的应用	
	18:00	**晚餐**	

报 告 简 介

Sol 3-流形的手征性与实二次算术

田野（中国科学院数学与系统科学研究院）

Sol 3-流形可由双曲整数矩阵描述，其特征方向给出周期连分数，并与不定二元二次型及实二次理想类密切相关。本报告将说明流形的手征性如何转化为类群中的反演对称，并介绍这一问题与 Pell 方程以及实二次数域在密码学中的应用之间的联系。

Post-quantum Cryptography, A New Era

丁津泰（西交利物浦大学）

Public key cryptosystems (PKC) are the security foundation of modern communication systems, in particular, the Internet. However Shor's algorithm shows that the existing PKC like Diffie-Hellmann key exchange, RSA and ECC can be broken by a quantum computer. To prepare for the coming age of quantum computing, we need to build new public key cryptosystems that could resist quantum computer attacks. In this lecture, we will give an introduction to post-quantum cryptography and its recent developments, in particular, the NIST standardization process and its impact. Then we will present a practical and provably secure key exchange protocol based on the learning with errors problems, which is conceptually simple and has strong provable security properties. We will explain final the current development in PQC and it migration.

MDS Array Codes: Theoretical Bounds and Practical Constructions

胡思煌（山东大学）

Maximum distance separable (MDS) array codes are fundamental to distributed storage systems, as they provide optimal fault tolerance for a given storage overhead. However, conventional MDS codes, such as Reed–Solomon codes, usually incur high repair bandwidth, whereas minimum storage regenerating (MSR) codes, despite being bandwidth-optimal, often require exponentially large sub-packetization, resulting in substantial disk I/O and computational overhead. Motivated by this tension between repair efficiency and implementation cost, in this talk we investigate MDS array codes from both theoretical and practical perspectives. On the theoretical side, we study the repair limits of $(k+2, k, 2)$ MDS array codes and establish tight lower bounds on the average minimum repair bandwidth and average minimum repair access for single-node failures. Our analysis relates repair schemes to point sets on the projective line and exploits the sharply 3-transitive action of $PGL_2(\mathbb{F}_q)$, leading to provable asymptotically tight lower bounds. On the practical side, we present a construction of MDS array codes obtained from a base MDS code by introducing only a small number of additional XOR operations. The resulting codes maintain low sub-packetization, support efficient encoding and single-node repair via standard base-code decoding, and achieve the proposed lower bound on repair access.

On permutation polynomials of index $q+1$ over $\mathbb{F}_{q^2}$

王强（Carleton University）

We give a survey on permutation polynomials over $\mathbb{F}_{q^2}$ with index $q+1$. In particular, we focus on some explicit classes of dense permutation polynomials with those indices, which are constructed from Rédei functions, or any permutation polynomials of $\mathbb{F}_q$, or injective mappings on the set μ_{q+1} of all $q+1$-th roots of unity.

The automorphism groups of random linear codes

王琦（南方科技大学）

The study of automorphism groups of linear codes is a fundamental topic in coding theory. The matching codewords framework is currently the standard tool for assessing the security of cryptographic schemes based on the hardness of the Linear Code Equivalence (LCE) problem, such as the LESS signature scheme and its variants. This framework often relies on the assumption that q-ary random codes have trivial automorphism groups. However, this assumption has not been formally proved in the literature. In this talk, we prove that with high probability, k-dimensional random linear codes $\mathcal{C} \subseteq \mathbb{F}_q^n$ have a trivial automorphism group as n goes to infinity as long as $min\{k, n-k\} \geq (2+\varepsilon)\log_q n$, for any $\varepsilon > 0$. This is joint work with Xiaoru Li and Yue Zhou.

Further results on bent partitions

王佳鑫（合肥工业大学）

Bent partitions of $V_n^{(p)}$ play an important role in constructing (vectorial) bent functions, partial difference sets, and association schemes, where $V_n^{(p)}$ denotes an n-dimensional vector space over the finite field $\mathbb{F}_p$, n is an even positive integer, and p is a prime. It is a challenging open problem whether the depth of any bent partition of $V_n^{(p)}$ is always a power of p. Notably, the depths of all currently known bent partitions of $V_n^{(p)}$ are powers of p. We prove that for a bent partition Γ of $V_n^{(p)}$ for which all the p-ary bent functions generated by Γ are regular or all are weakly regular but not regular, the depth of Γ must be a power of p. We present new constructions of bent partitions that (do not) correspond to vectorial dual-bent functions. In particular, a new construction of vectorial dual-bent functions is provided. Additionally, for general bent partitions of $V_n^{(2)}$, we establish a characterization in terms of Hadamard matrices.

Several famous conjectures related to polynomials representing primes

秦厚荣（南京大学）

Dirichlet's density theorem answers the question of prime representation by linear polynomials. Whether a quadratic polynomial can represent primes infinitely often-for example, Euler's conjecture that x^2+1 can represent primes infinitely often-is notoriously difficult and remains wide open. More generally, the Hardy-Littlewood conjecture gives an asymptotic formula for the count of such primes. In parallel, for an elliptic curve E over $\mathbb{Q}$ with complex multiplication (CM) and a fixed nonzero integer r, the Lang–Trotter conjecture predicts an asymptotic formula for $\pi_{E,r}(x)=\#\{p\le x: a_p=r\}$, where a_p is the Frobenius trace. We introduce a new invariant, the CM conductor $\mathcal{K}_E$, which refines the Serre conductor in the CM case. Using $\mathcal{K}_E$, we give a corrected formula for the Lang–Trotter constant$c_{E,r}$, differing from the previous one by Baier and Jones. Assuming the Hardy–Littlewood conjecture on quadratic polynomial primes, we prove that our version of the Lang–Trotter conjecture holds for every CM elliptic curve over $\mathbb{Q}$. We compute the constants explicitly for each imaginary quadratic field of class number one, characterize exactly when the constant vanishes, and prove the conjecture unconditionally in the vanishing case. Numerical evidence strongly supports our formulation. This is joint work with Longxi Hu and Kaisheng Lei.

A Structural Characterization of Cyclotomic Cosets with Applications to Affine-Invariant Codes and BCH Codes

郑大彬（湖北大学）

Affine-invariant codes have attracted considerable attention due to their rich algebraic structure and strong theoretical properties. In this paper, we study a family of affine-invariant codes whose defining set consists of all descendants of elements in the cyclotomic coset of a single specified element. Our main contributions are as follows. First, we establish a new combinatorial result that determines exactly the size of such descendant sets, which is of independent interest in the study of cyclotomic cosets. Second, using this result, we derive explicit formulas for the dimensions of the corresponding affine-invariant codes and their associated cyclic codes, and we establish lower bounds on the minimum distances of their duals. In particular, under appropriate parameter choices, these codes yield narrow-sense primitive BCH codes and their extended counterparts. For the special class of narrow-sense primitive BCH codes with designed distance $\delta = (b+1)q^{m-t-1}$, where $1 \le b \le q-1$ and $0 \le t \le m-1$, we provide exact dimension formulas and an improved lower bound on the minimum distance. The results presented here extend and sharpen several previously known results, and provide refined tools for the parametric analysis of BCH codes and their duals.

On the Niho type locally-APN power functions and their boomerang spectrum

李念（湖北大学）

In this talk, we focus on the concept of locally-APN-ness introduced by Blondeau, Canteaut, and Charpin, which makes the corpus of S-boxes somehow larger regarding their differential uniformity and, therefore, more suitable candidates against the differential attack (or their variants). Specifically, given two coprime positive integers m and k such that $\gcd(2^m+1,2^k+1)=1$, we investigate the locally-APN-ness property of an infinite family of Niho type power functions in the form $F(x)=x^{s(2^m-1)+1}$ over the finite field $\mathbb{F}_{2^n}$ for $s=(2^k+1)^{-1}$, where $(2^k+1)^{-1}$ denotes the multiplicative inverse modulo 2^m+1. By employing finer studies of the number of solutions of certain equations over finite fields (with even characteristic) as well as some subtle manipulations of solving some equations, we prove that $F(x)$ is locally APN and determine its differential spectrum. It is worth noting that computer experiments show that this class of locally-APN power functions covers all Niho type locally-APN power functions for $2\leq m\leq 10$. In addition, we also determine the boomerang spectrum of $F(x)$ by using its differential spectrum, which particularly generalizes a recent result by Yan, Zhang, and Li.

唯一可译的网络函数计算编码

光炫（南开大学）

Uniquely-decodable coding for zero-error network function computation will be introduced in this talk, where in a directed acyclic graph, the single sink node is required to compute with zero error a target function multiple times, whose arguments are the information sources generated at source nodes. We are interested in the computing capacity from the information theoretic point of view, which is defined as the infimum of the maximum expected number of bits transmitted on all the edges for computing the target function once on average. We first prove some new results on clique entropy, in particular, the substitution lemma of clique entropy for probabilistic graphs with a certain condition. With them, we prove a lower bound on the computing capacity associated with clique entropies of the induced characteristic graphs, where the obtained lower bound is applicable to arbitrary network topologies, arbitrary information sources, and arbitrary target functions. By refining the probability distribution of information sources, we further strictly improve the obtained lower bound. In addition, we compare uniquely-decodable network function-computing coding and fixed-length network function-computing coding, and show that the former indeed outperforms the latter in terms of the computing capacity.

Good families of binary sequences with low correlation and high linear complexity via function fields

马立明（中国科学技术大学）

In the realm of modern digital communication, cryptography, and signal processing, binary sequences with good correlation properties play a pivotal role. In the literature, considerable efforts have been dedicated to constructing good binary sequences of various lengths. As a consequence, numerous constructions of good binary sequences have been put forward. However, the majority of known constructions leverage the multiplicative cyclic group structure of finite fields $\mathbb{F}_{p^n}$, where p is a prime and n is a positive integer.

First, we made use of the cyclic group structure of all rational places of the rational function field over the finite field $\mathbb{F}_{p^n}$, and constructed good binary sequences of length p^n+1 via cyclotomic function fields over $\mathbb{F}_{p^n}$ for any prime p. This approach has paved a new way for constructing good binary sequences. Motivated by the above constructions, we exploit the cyclic group structure of rational points of elliptic curves to design a family of binary sequences of length 2^n+1+t with low correlation for many given integers $|t| \le 2^{(n+2)/2}$. Specifically, for any positive integer d with $\gcd(d, 2^n+1+t)=1$, we introduce a novel family of binary sequences of length 2^n+1+t, size $q^{d-1}-1$, correlation bounded by $(2d+1)\cdot 2^{(n+2)/2}+|t|$, and large linear complexity via elliptic curves. Finally, we provide a framework of constructing multi-sequences with high linear complexity via function fields and give many interesting families of multi-sequences.

基于同源的后量子密码体系

欧阳毅（中国科学技术大学）

基于同源的密码体系是后量子密码学一条技术路径。本报告将介绍同源密码和它依赖的数学困难问题，然后介绍我们在超奇异同源图结构和 SQI 签名方案方面的一些研究成果，基于和徐铮、李宋宋、周子健、林楷展、赵昌安等的合作研究。

Locally Repairable Codes with Availability via Elliptic Function Fields

赵昌安（中山大学）

Locally repairable codes with availability have become essential components in modern large-scale distributed cloud storage systems and numerous other applications. In this paper, we focus on the construction of locally repairable codes with one or two recovering sets via elliptic function fields. Prior pioneering work by Li et al. (IEEE Trans. Inf. Theory, vol. 65, no. 1, 2019) and Ma and Xing (J. Comb. Theory Ser. A., vol. 193, 2023) employed maximal supersingular elliptic curves to obtain several optimal (classical) locally repairable codes. In contrast, we consider ordinary elliptic curves with many rational points. This approach yields several new families of q-ary optimal locally repairable codes with length $O(q+2\sqrt{q})$ and flexible locality. Consequently, our work broadens the selection of curves available for the construction of optimal locally repairable codes.

Furthermore, we present a general framework for constructing locally repairable codes with two recovering sets via automorphism groups of elliptic function fields. To realize this framework, we devise a novel construction for determining the functions e_i in the construction of locally repairable codes. By employing both supersingular and ordinary elliptic curves, we obtain several families of locally repairable codes with two recovering sets. In particular, we construct a family of q^2-ary locally repairable codes with two recovering sets, achieving length $O(q^2+2q)$ and Singleton-defect $O\left(\frac{2\ell}{q^2+2q-8\ell}\right)$, where $\ell \parallel q+2$ with $4\ell < q$.

A Novel Leakage Model in OpenSSL's Miller-Rabin Primality Test

胡红钢（中国科学技术大学）

At CRYPTO 2009, Heninger and Shacham presented a branch-and-prune algorithm for reconstructing an RSA private key given a random fraction of its private components. This method has been widely adopted in side-channel attacks, and its complexity is closely related to the specific leakage pattern encountered. In this work, we propose a new leakage model that enables efficient key reconstruction by exploiting a vulnerability in the modular exponentiation invoked by OpenSSL's implementation of Miller-Rabin primality test. This vulnerability reveals the least significant b bits of each window. Through our proposed model, these bits form new leakage patterns, which we term aligned and misaligned. In particular, the misaligned case includes previously undocumented scenarios where full key recovery is achievable without branching. Then we analyze the global and local behavior of key reconstruction under these patterns. Our evaluation demonstrates that they yield more efficient key reconstruction and maintain this advantage even in the presence of additional erasures. Moreover, in specific scenarios, successful reconstruction remains practical even if the bits obtained are less than 50%. Finally, we conducted a series of experiments to confirm the practicality of our work, successfully recovering the lower 4 bits from each 6-bit window and demonstrating efficient key reconstruction under our model.