Titles and Abstracts

1. Xiwang Cao, Nanjing University of Aeronautics and Astronautics, China
   Title: Optimal p-ary cyclic codes with minimum distance four from monomials
   Abstract: In this talk, we show some constructions of optimal p-ary cyclic codes $\mathcal{C}_{(0,1, e)}$ with parameters $[p^m-1,p^m-2m-2, 4]$ from perfect nonlinear monomials and the inverse function over $\mathbb{F}_{p^m}$. We focus on the quinary cyclic codes $\mathcal{C}_{(1, e)}$ and $\mathcal{C}_{(0,1, e)}$, where $e\notin\Gamma_1$ and $\mid \Gamma_e\mid=m$. We will show that the minimum distance of quinary cyclic codes $\mathcal{C}_{(1, e)}$ is equal to 2 or 3 depending on whether e is odd or e is even. To obtain optimal quinary cyclic codes, we investigate a class of subcodes of $\mathcal {C}_{(1,e)}$ and employ some known almost perfect nonlinear monomials and other monomials over $\mathbb{F}_{5^m}$ to construct optimal quinary cyclic codes $\mathcal{C}_{(0, 1, e)}$ with parameters $[5^m-1,5^m-2m-2, 4]$.
   This is a joint work with Dr. Guangkui Xu.

2. Yonglin Cao, Shandong University of Technology, China
   Title: Constacyclic codes over $F_{p^m} + uF_{p^m}$ of length $p^s n$
   Abstract: Dinh et al. [Finite Fields Appl., **31** (2015)] studied negacyclic codes of length $2p^s$ over the ring $F_{p^m} + uF_{p^m}$. Chen et al. [Finite Fields Appl. **37** (2016)] investigated constacyclic codes of length $2p^s$ over the ring $F_{p^m} + uF_{p^m}$. The main result and their proofs depend heavily on the code length $2p^s$.

   Let $R = F_{p^m} + uF_{p^m}$ ($u^2 = 0$), n, s be arbitrary positive integers satisfying $\gcd(p,n) = 1$, and $\lambda = \alpha + u\beta$ where $\alpha,\beta \in F_{p^m}$ and $\alpha \neq 0$. Then λ-constacyclic codes over R of length $p^s n$ are identified with ideals of the residue class ring $R[x]/\langle x^{p^s n} - \lambda\rangle$. When $\beta \neq 0$, $R[x]/\langle x^{p^s n} - \lambda\rangle$ is a principal ideal ring. When $\beta=0$, using known results for linear codes over finite chain rings and by matrix theory over finite chain rings, we provide a new way to determine the algebraic structures, the generators and enumeration for all ideals of $R[x]/\langle x^{p^s n} - \lambda\rangle$.

   Specifically, the following questions are addressed: (i) Give a precise representation for each λ-constacyclic code C over R of length $p^s n$, and provide a simple and clear formula to count the number of codewords in C. (ii) Give a clear formula to count the number of all λ-constacyclic codes over R of length $p^s n$. (iii) Give a precise representation for the dual code of each λ-constacyclic code C over R of length $p^s n$, once the representation of C is given. (iv) Determine self-dual negacyclic codes over R of length $p^s n$.

3. Yingpu Deng, Academy of Mathematics and Systems Sciences, CAS, China

Title: Algorithm for computing the factor ring of an ideal in Dedekind domain with finite rank

Abstract: We give an algorithm for computing the factor ring of a given ideal in a Dedekind domain with finite rank, which runs in deterministic and polynomial-time. We provide two applications of the algorithm: deciding whether a given ideal is prime or prime power. The main algorithm is based on basis representation of finite rings which are computed via Hermite and Smith normal forms.

4. Fangwei Fu, Nankai University, China

   Title: The List Decoding Error Probability of Linear Codes over the Erasure Channel

   Abstract: In this paper, we study the list decoding error probability of a linear code over the erasure channel. The notion of L-incorrigible sets of a linear code is introduced to characterize its performance under list decoding. The L-incorrigible set distribution of a linear code can also be used to completely determine its decoding error probability under maximum likelihood decoding over the erasure channel. Furthermore, we show that the L-incorrigible set distribution of a linear code can be determined by its support weight distribution. Finally, the error exponent of the unsuccessful decoding probability under optimal decoding for the ensemble of all $[n, nR]$ linear codes is determined. This is a joint work with Lin-Zhi Shen.

5. Gennian Ge, Capital Normal University, China

   Title: Separating hash families: A Johnson-type bound and new constructions

   Abstract: Separating hash families are useful combinatorial structures which are generalizations of many well-studied objects in combinatorics, cryptography and coding theory. In this talk, using tools from graph theory and additive number theory, we solve several open problems and conjectures concerning bounds and constructions for separating hash families, which include: Bazrafshan-Trung's open problem on separating hash families, Alon-Stav's conjecture on parent-identifying codes, and Walker II-Colbourn's conjecture on perfect hash families. In addition, we also approve partially aquestion of Blackburn-Etzion-Stinson-Zaveruchaa on perfect hash families.

6. Hongwei Liu, Central China Normal University, China

   Title: Homogeneous Weights of Matrix Product Codes over Finite Principal Ideal Rings.

   Abstract: The notion of matrix product code was first introduced by Blackmore and Norton in 2001. It is a generalization of some well known constructions of codes over finite fields, e.g., (u|u+v)-construction, (a+x|b+x|a+b+x)-construction, (u + v + w|2u + v |u)-construction and etc. In this talk, we study the homogeneous weights of matrix product codes over finite principal ideal rings, and we obtain a lower bound for the minimum homogeneous weights of such

matrix product codes. This is a joint work with Professor Yun Fan and Professor San Ling.

7. Jinquan Luo, Central China Normal University, Wuhan, China
   Title: Constant composition codes from cyclic codes
   Abstract: Constant composition codes are codes where the frequency distribution of the elements in a codeword is the same for all codewords.In this talk several classes of constant composition codes will be introduced. These codes are subcodes of cyclic codes which have few weights occurring among the codewords. The new codes are excellent asymptotically compared to the previously best known constant composition codes.

8. Lei Hu, Chinese Academy of Sciences, China
   Title: Modular Inversion Hidden Number Problem Revisted
   Abstract: In this talk we revisit the modular inversion hidden number problem and a related random number generator-the inversive congruential pseudo random number generator, and consider how to more efficiently attack them in terms of fewer samples or output bits. We reduce the problem to finding small solutions of systems of modular polynomial equations of the form $a_i + b_i x_0 + c_i x_i + x_0 x_i = 0 (mod\ p)$, and present two strategies to construct lattices for the solving of the equations. Different from the choosing of the polynomials used for lattice constructions in previous methods, a part of polynomials chosen in our strategies are linear combinations of some polynomials generated in advance and this enables us to achieve a larger upper bound for the desired root. Applying this technique to the modular inversion hidden number problem, we put forward an explicit result of Boneh et al and give an improvement in the involved lattice construction in the sense of requiring fewer samples. Our strategies also gives a method of attacking the inversive congruential pseudo random number generator, and the corresponding result is the best up to now. This is a joint work with Jun Xu, Zhangjie Huang and Liqiang Peng.

9. Ming-Deh Huang, University of Southern California
   Title: Last fall degrees of Weil descent systems and cryptography
   Abstract: Recent developments concerning applications of Weil descent in cryptographic settings raised interesting complexity theoretic questions about the Weil descent of affine algebraic systems .
   In this talk we will discuss theoretical works centering on the notion of last fall degrees of polynomial systems, and their applications to multivariate public key cryptography and elliptic curve cryptography.

10. Lingfei Jin, Fudan University, China
    Title: Multipartite entangled states, symmetric matrices and error-correcting codes
    Abstract: A pure quantum state is called *k*-uniform if all its reductions to *k*-qudit are maximally mixed. We investigate the general constructions of *k*-uniform pure

quantum states of n subsystems with d levels. We provide one construction via symmetric matrices and the second one through classical error-correcting codes. There are three main results arising from our constructions. Firstly, we show that for any given even $n \geq 2$, there always exists an $n/2$-uniform n-qudit quantum state of level p for sufficiently large prime p. Secondly, both constructions show that their exist k-uniform n-qudit pure quantum states such that k is proportional to n, i.e., $k = \Omega(n)$ although the construction from symmetric matrices outperforms the one by error-correcting codes. Thirdly, our symmetric matrix construction provides a positive answer to the open question on whether there exists 3-uniform n-qudit pure quantum state for all $n \geq 8$.

11. Longjiang Qu, National University of Defense Technology, China
    Title: A New Approach to Construct Quadratic Pseudo-Planar Functions over F_2^n
    Abstract: Planar functions over finite fields give rise to finite projective planes. They were also used in the constructions of DES-like iterated ciphers, error-correcting codes, and codebooks. They were originally defined only in finite fields with odd characteristic, but recently Zhou introduced pesudo-planar functions in even characteristic which yields similar applications. All known pesudo-planar functions are quadratic and hence they give presemifields. In this paper, a new approach to construct quadratic pseudo-planar functions is given. Then five explicit families of pseudo-planar functions are constructed, one of which is a binomial, two of which are trinomials, and the other two are quadrinomials. All known pesudo-planar functions are revisited, some of which are generalized. These functions not only lead to projective planes, relative difference sets and presemifields, but also give optimal codebooks meeting the Levenstein bound, complete sets of mutually unbiased bases (MUB) and good compressed sensing matrices.

12. MinJia Shi, Anhui University, China
    Title: Quasi-twisted codes with constacyclic component codes
    Abstract: Quasi-twisted codes are generalizations of the familiar linear quasi-cyclic codes. In this paper, we apply an algebraic method to investigate the relationship between quasi-twisted codes constacyclic codes. Moreover, a generator polynomial of a quasi-twisted code with constacyclic component codes is given. Meanwhile, we obtain the necessary conditions for a quasi-twisted code $\mathscr{C}$ of index ℓ and length ℓm to be equivalent to a constacyclic code of length ℓm. Finally, some examples are presented to illustrate the discussed results.

13. Xiaohu Tang, Southwest Jiaotong University, Chengdu, China
    Title: Placement-Delivery Array and Its construction for Caching based Communication Systems
    Abstract: Caching is a promising solution to satisfy the ever-increasing demands for the multi-media traffics. In caching networks, coded caching is a recently proposed technique that achieves significant performance gains over the uncoded

caching schemes. In this talk, we will first review the background of coded caching and its model. Next, we will introduce a combinatorial structure called placement-delivery array to describe the coded caching. Finally, we will present a construction for PDA.

14. Dianhua Wu, Guangxi Normal University, China
    Title: Recent Progress on Optimal Optical Orthogonal Codes
    Abstract: Optical orthogonal codes (OOCs) were introduced by Salehi, as signature sequences to facilitate multiple access in optical fibre networks. OOCs had been found wide ranges of applications such as mobile radio, frequency-hopping spread-spectrum communications, radar, sonar, collision channel without feedback and neuromorphic networks. In 1996, Yang introduced variable-weight optical orthogonal code (VWOOC) for multimedia optical CDMA systems with multiple quality of service (QoS) requirements. In this talk, recent progress on OOCs, especially, the VWOOCs, will be presented.

15. Huaxiong Wang, Nanyang Technological University, Singapore
    Title: Secure Multiparty Computation: Past and Present
    Abstract: Secure Multiparty computations (MPC) are basic cryptographic protocols that allow a group of mutually distrusting parties to evaluate a function for their private inputs in such a way that the group knows the outcome of the computation while their inputs stay private. In this talk, we give a survey of the-state-of-art in secure MPC.

16. Qi Wang, Southern University of Science and Technology, China
    Title: Explicit construction of LDPC codes based on the space of symmetric matrices over F_q
    Abstract: Based on Sn(F_q), the space of $n\times n$ symmetric matrices over F_q, we give an explicit construction of regular LDPC codes. Via this construction, we obtain two classes of regular LDPC codes, $C(n, q)$ and C^T (n, q), whose corresponding sparse bipartite graph has girth 8. We study both the minimum distance and the stopping distance of these two classes of LDPC codes, and give explicit results for some cases and lower bounds for others.
    This is joint work with Meng Zhao and Changli Ma.

17. Qiang Wang, Carleton University, Canada
    Title: On Compositional Inverses of Permutation Polynomials Over Finite Fields
    Abstract: The problem of determining the compositional inverse of a permutation polynomial over finite fields seems to be a challenging problem. In fact, there are very few known permutation polynomials whose explicit compositional inverses have been obtained, and the resulting expressions are usually of a complicated nature except for those well known classes. We survey these known results and current prgress on the inverses of permutation polynomials.

18. Wenling Wu, Institute of Software, Chinese Academy of Sciences, China
    Title: Constructing Lightweight Optimal Diffusion Layers
    Abstract: Diffusion layer is one of the core components in a block cipher with confusion layer. And it is also widely used in many other block cipher-based primitives, for instance, hash functions. The choice of a diffusion layer influences both the security and efficiency of a cryptographic primitive. On the one hand, it plays an important role in providing security against differential cryptanalysis and linear cryptanalysis, which are the two most important cryptanalysis of block ciphers. On the other hand, with the same security, an elaborate diffusion layer may lead to a better performance of a cryptographic primitive on hardware or/and software implementation. The strength of a diffusion layer is usually measured by the notation of branch number. A block cipher using a diffusion layer with small branch number may suffer unexpected attacks. Therefore, how to construct a diffusion layer with big branch number and low-cost implementation is a challenge for designers. In this talk, we first propose a new class of lightweight optimal diffusion layers constructed by Feistel structure with bit permutation as round functions. Then, we construct recursive diffusion layers using Linear Feedback Shift Registers, and investigate the sufficient and necessary condition that make such diffusion layers perfect.

19. Maosheng Xiong, Hong Kong University of Science and Technology, Hong Kong
    Title: Construction of Unit-Memory MDS Convolutional Codes
    Abstract: Maximum-distance separable (MDS) convolutional codes form an optimal family of convolutional codes, the study of which is of great importance. There are very few general algebraic constructions of MDS convolutional codes. In this talk, we construct a large family of unit-memory MDS convolutional codes over $\F_q$ with flexible parameters. Compared with previous works, the field size q required to define these codes is much smaller. The construction also leads to many new strongly-MDS convolutional codes, an important subclass of MDS convolutional codes which was proposed and studied in 2006. We will present many examples at the end.

20. Maozhi Xu, Peking University, China
    Title: Solving the Elliptic Curve Discrete Logarithm Problem on some Supersingular Elliptic Curves
    Abstract: In 2013 and 2014 there have been several announcements that the computation of discrete logarithms in small characteristic finite fields has been greatly improved. For example, Robert Granger, Faruk Göloğlu, Gary McGuire, and Jens Zumbragel solved a new example in the field $F_{2^{6120}}$. If some elliptic curves can be embedded into these finite field, there will have fast algorithms to solve this ECDLP. In this talk we summarize the constructions of supersingular elliptic curves over finite field of characteristic 2 and 3. We also build some supersingular elliptic curves with a prime order subgroup of cardinality of bitlength larger than 200-bit(the largest case is1536-bit), these special ECDLP are

relatively easy to be solved by MOV attack. Examples of such elliptic curves are:

Embedding degree k=3:

$$\mathrm{E}/\mathrm{F}_{2^{257*2}}: y^2 + a \cdot \mathrm{y} = x^3 + a^{513}, \text{ a is a generator of } F^*_{2^{257*2}}$$

Embedding degree k=4:

$$\mathrm{E}/\mathrm{F}_{2^{257}}: y^2 + \mathrm{y} = x^3 + x,$$
$$\mathrm{E}/\mathrm{F}_{2^{257}}: y^2 + \mathrm{y} = x^3 + x + 1,$$

Embedding degree k=2:

$$\mathrm{E}/\mathrm{F}_{2^{3060}}: y^2 + \mathrm{y} = x^3 + a^3, \text{ a is a generator of } F^*_{2^{1020*2}}$$

Embedding degree k=3:

$$\mathrm{E}/\mathrm{F}_{2^{1020*2}}: y^2 + a \cdot \mathrm{y} = x^3 + a^{2035}, \text{ a is a generator of } F^*_{2^{1020*2}}$$
$$\mathrm{E}/\mathrm{F}_{2^{204*2}}: y^2 + a \cdot \mathrm{y} = x^3 + a^5, \text{ a is a generator of } F^*_{2^{204*2}}$$

Embedding degree k=2:

$$\mathrm{E}/\mathrm{F}_{2^{1537}}: y^2 + \mathrm{y} = x^3$$

Embedding degree k=3:

$$\mathrm{E}/\mathrm{F}_{2^{513*2}}: y^2 + a \cdot \mathrm{y} = x^3 + a^{513}, \text{ a is a generator of } F^*_{2^{257*2}}$$

Embedding degree k=1:

$$\mathrm{E}/\mathrm{F}_{3^{163*2}}: y^2 = x^3 + x,$$

Embedding degree k=3:

$$\mathrm{E}/\mathrm{F}_{3^{163*2}}: y^2 = x^3 + a^2\mathrm{x} + a^8, \text{ a is a generator of } F^*_{3^{163*2}}$$

Embedding degree k=6:

$$\mathrm{E}/\mathrm{F}_{3^{163}}: y^2 = x^3 - x - a^5, \text{ a is a generator of } F^*_{3^{163}}$$
$$\mathrm{E}/\mathrm{F}_{3^{163}}: y^2 = x^3 - x + a^5, \text{ a is a generator of } F^*_{3^{163}}$$

21. Qing Xiang, University of Delaware, USA

Title: A New Infinite Family of Hemisystems of the Hermitian Surface

Abstract: We will talk about a recent construction of an infinite family of hemisystems of the Hermitian surface $H(3, q^2)$. In particular, we show that for every odd prime power q congruent to 3 modulo 4, there exists a hemisystem of $H(3, q^2)$ admitting $C_{(q^3+1)/4}: C_3$. The talk is based on joint work with John Bamberg, Melissa Lee, and Koji Momihara.

22. Lin You, Hangzhou Dianzi University, China

Title: Algebraic Curve Pseudorandom Sequences Over Finite Fileds

Abstract: Algebraic curves over finite fields have been widely applied for constructing cryptography, such as elliptic curve cryptography and hyperelliptic curve cryptography, and they have also been used for constructing algebraic geometrical codes. Moreover, we can employ algebraic curves over finite fields to construct pseudorandom sequences for stream ciphers. In this talk, we will give a survey about the constructions of pseudorandom sequences from algebraic curves over finite fields, and discuss their periods, linear complex and correlation.

23. Zhifang Zhang, Academy of Mathematics and Systems Science, China
    Title: An integer programming based bound for locally repairable codes
    Abstract: The locally repairable code (LRC) discussed in this paper is an [n, k] linear code of which the value at each coordinate can be recovered by a linear combination of at most r other coordinates. The central problem in this talk is to determine the largest possible minimum distance for LRCs. Specifically, a tight bound on the minimum distance is derived for a wide region of parameters.

24. Yue Zhou, National University of Defense Technology, China
    Title: Generalized Twisted Gabidulin codes
    Abstract: Recently, J. Sheekey constructed a new family of maximum rank distance codes as sets of q-polynomials over GF(q^n), which are called the twisted Gabidulin codes. In this talk, we look at a generalization of them, which we call generalized twisted Gabidulin codes. Their Delsarte duals and adjoint codes are considered. We also completely determine the equivalence between different members of the generalized twisted Gabidulin codes, from which it follows that the generalized Gabidulin codes and the twisted Gabidulin codes are both proper subsets of this new family.

25. Yan Zhu, University of Science and Technology Beijing, China
    Title: How to design a secure aggregation code for perfect group-based encryption
    Abstract: In this presentation, we will explore how to implement cryptographic positive and negative membership predicates. Based on these two predicates, it is easy to design perfect group-based encryption, such as, identity-set-based encryption and attribute-set-based encryption. The core of our schemes is the implementation of cryptographic representation of subset by using two aggregation codes: Zeros-based aggregation and Poles-based aggregation. These two aggregation functions are capable of compressing any subset into one element in a bilinear map group for determining the membership between an element and a subset. Our scheme achieves the optimal bound of O(1)-size for either ciphertext (consisting of just two elements) or decryption key (one element) for an identity set of large size. We prove that our scheme is secure under the General Die-Hellman Exponent (GDHE) assumption.