The 1st International Coding Theory Seminar

China (online)

December 1st, 2023

Contents

About

Organizing committee

China
Xiwang Cao
Lingfei Jin (vice chair)
Hongwei Liu (chair)
Gaojun Luo

India
Manish Gupta (chair)
Sartaj Ul Hasan
Anuradha Sharma

Japan
(TBA)

Korea
Whan-Hyuk Choi
Boran Kim
Jon-Lark Kim (chair)

Philippines
Rowena Betty
Romar dela Cruz
Lucky Galvez (chair)

Thailand
Arunwan Boripan
Parinyawat Choosuwan
Somphong Jitman (chair)
Ekkasit Sangwisut

Singapore
Han Mao Kiah (chair)

International advisors

Nathan Kaplan (USA)

Patrick Sole (France)

Hong-Yeop Song (Korea)

Chaoping Xing (China)

Timetable

All times listed are in Beijing Standard Time (GMT+8).

Time: December 1st, 2023

Zoom ID: 275 839 8498

Password: 3bMnxY

13:00-14:00	**Committee Discussion**	
14:00–14:40	**Yongbo Xia** Wuhan, China	The Differential Spectra of Some Cryptographic Functions with Low Differential Uniformity
14:40–15:00	**Discussion**	
15:00–15:40	**Weijun Fang** Qingdao, China	Some Topics on Locally Repairable Codes
15:40–16:00	**Discussion**	
16:00–16:10	**Break**	
16:10–16:50	**Liming Ma** Hefei, China	An Introduction to Algebraic Geometry Codes and Related Topics
16:50–17:10	**Discussion**	

List of Talks

Talk 1: The Differential Spectra of Some Cryptographic Functions with Low Differential Uniformity

Yongbo Xia

Department of Mathematics and Statistics,
South-Central University for Nationalities, Wuhan 430074, China
xia@mail.scuec.edu.cn

Biography
Yongbo Xia received the B.S., M.S., and Ph.D. degrees in mathematics from the Department of Mathematics, Hubei University, Wuhan, China, in 2003, 2006, and 2009, respectively. From September 2013 to September 2014, he was a Visiting Researcher with the Department of Informatics, University of Bergen, Norway. Since 2006, he has been with the Department of Mathematics and Statistics, South-Central University for Nationalities, Wuhan, where he is currently a Professor. His research interests include sequence design for wireless communication, coding theory, and cryptography. Differential property is one of the most important metrics of cryptographic functions used in symmetric cryptography. More specifically, the differential uniformity quantifies the security of the mappings used in block ciphers with respect to the powerful differential cryptanalysis. The lower the differential uniformity of a function, the more resilient it is to differential cryptanalysis if used in a substitution box.

Abstract
Compared to the differential uniformity, the differential spectrum of a cryptographic function reflects more information about its differential property. The differential spectrum of a function can be used to analyze its resistance against some variants of differential cryptanalysis, especially the truncated differential attacks. In addition to its importance in cryptography, the differential spectrum of a nonlinear mapping also plays a significant role in sequences, coding theory and combinatorial design. A complete investigation on the differential spectrum of a given function is interesting yet challenging in general.

Our talk will introduce the research progresses in this area, including the following topics:

- an overview of previously known results,
- the commonly-used methods for computing the differential spectra,
- new results about the differential spectra of some power mappings and some binomials with low differential uniformity.

Open problems and some related research topics will also be discussed, which are given as follows:

- computing the differential spectra of other power mappings, especially, the APN power mapping over finite fields of odd characteristic,
- calculating the differential spectra of other mappings, which are not power mappings,
- investigating the c-differential spectrum, DDT, boomerang spectrum, BCT, DLCT of cryptographic functions,
- finding some applications of the differential spectrum (DDT, boomerang spectrum, BCT etc.) in cryptography and coding theory.

Bibiography

[1] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3-72, 1991.

[2] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in cryptology-EUROCRYPT'93 (Lecture Notes in Computer Science)*, vol. 765, T. Helleseth Eds. Berlin, Germany: Springer-Verlag, 1994, pp. 55-64.

[3] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of power functions," *Int. J. Inf. Coding Theory*, vol. 1, no. 2, pp. 149-170, 2010.

[4] C. Blondeau, A. Canteaut, and P. Charpin, "Differential properties of $x \mapsto x^{2^t-1}$," *IEEE Trans. Inf. Theory*, vol. 57, no. 12, pp. 8127-8137, 2011.

[5] C. Blondeau and L. Perrin, "More differentially 6-uniform power functions," *Des. Codes Cryptogr.*, vol. 73, no. 2, pp. 487-505, 2014.

[6] T. Helleseth and D. Sandberg,"Some Power Mapping with Low Differential Uniformity," *Applicable Algebra in Engineering, Communication and Computing*, vol. 8, pp. 363-370, 1997.

[7] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 475-485, 1999.

[8] G. J. Ness and T. Helleseth, "A new family of ternary almost perfect nonlinear mappings," *IEEE Trans. Inf. Theory*, vol. 53, no. 7, pp. 2581-2586, 2007.

[9] S. T. Choi, S. Hong, J. S. No, and H. Chung, "Differential spectrum of some power functions in odd prime characteristic," *Finite Fields Appl.*, vol. 21, pp. 11-29, 2013.

[10] M. Xiong and H. Yan, "A note on the differential spectrum of a differentially 4-uniform power function," *Finite Fields Appl.*, vol. 48, pp. 117-125, 2017.

[11] M. Xiong, H. Yan, and P. Yuan, "On a conjecture of differenially 8-uniform power functions," *Des. Codes Cryptogr.*, vol. 86, no. 8, pp. 1601-1621, 2018.

[12] H. Yan, Z. Zhou, J. Weng, J. Wen, T. Helleseth, and Q. Wang, "Differential spectrum of Kasami power permutations over odd characteristic finite fields," *IEEE Trans. Inf. Theory*, vol. 65, no. 10, pp. 6819-6826, 2019.

[13] Y. Xia, X. Zhang, C. Li and T. Helleseth, "The differential spectrum of a ternary power mapping", *Finite Fields Appl.*, vol. 64, 2020.

[14] H. Yan, Y. Xia, C. Li, T. Helleseth, M. Xiong, and J. Luo, "The differential spectrum of the power mapping x^{p^n-3}," *IEEE Trans. Inf. Theory*, vol. 68, no. 8, pp. 5535 - 5547, 2022.

[15] S. Jiang, K. Li, Y. Li, and L. Qu, "Differential and boomerang spectrums of some power permutations," *Cryptogr. Commun.*, vol. 14, no. 2, pp. 371-393, 2022.

[16] Y. Man, Y. Xia, C. Li, and T. Helleseth, "On the differential properties of the power mapping x^{p^m+2}," *Finite Fields Appl.*, vol. 84, no. 10, pp. 1-22, 2022.

[17] Z. Hu, N. Li, L. Xu, X. Zeng, and X. Tang, "The differential spectrum and boomerang spectrum of a class of locally-APN functions," *Des. Codes Cryptogr.*, vol. 91, no. 5, pp. 1695-1711, 2023.

[18] Y. Xia, F. Bao, S. Chen, C. Li, and T. Helleseth,"More Differential Properties about the Ness-Helleseth Nonlinear Mapping," submitted to *IEEE Trans. Inf. Theory*, 2023.

[19] Y. Xia, F. Bao, S. Chen, C. Li, and T. Helleseth, "A Direct Method for Calculating the Differential Spectrum of an APN Power Mapping," submitted to *Des. Codes Cryptogr.*, 2023.

Talk 2: Some Topics on Locally Repairable Codes

Weijun Fang

School of Cyber Science and Technology,
Shandong University, Qingdao, 266237, China
fwj@sdu.edu.cn

Biography
Weijun Fang received the B.S. degree in mathematics and the Ph.D. degree in probability and mathematical statistics from Nankai University, Tianjin, China, in 2013 and 2019, respectively. From 2019 to 2021, he served as a Post-Doctoral Researcher with the Tsinghua Shenzhen International Graduate School, Tsinghua University, Shenzhen, China. Since September 2021, he has been a Research Fellow at the School of Cyber Science and Technology, Shandong University, Qingdao, China. He has authored over twenty academic papers, which have been published in distinguished journals and conferences such as TIT, TCOM, DCC, FFA, ISIT, and ITW. His current research interests include classical coding theory, quantum coding, and coding for distributed storage systems.

Abstract
To minimize the number of storage nodes to be downloaded, locally repairable codes (LRCs) were designed by Gopalan et al. These codes aim to recover a failed node by accessing fewer available nodes. The number of helper nodes required to reconstruct a failed node is referred to as the locality of the code.

Compared to replication codes, locally repairable codes offer improved storage efficiency, leading to significant reductions in storage costs for large-scale distributed storage systems. In contrast to MDS codes, which lack locality, locally repairable codes require only a small number of helper nodes when repairing a single node. The design of LRCs with high code rates, substantial minimum distances, and minimal locality is a desirable objective. However, these parameters are subject to specific constraints, such as the Singleton-type bound, the C-M bound, and the Hamming-type bound. Recent years, constructing optimal LRCs that meet these theoretical bounds is a critical area of focus in coding theory. From a practical standpoint, exploring fast encoding and decoding algorithms for locally repairable codes represents an engaging and challenging field of study.

This talk will introduce the research progresses in this area, including the following topics:

- An introduction tof LRCs,
- Bounds and constructions of optimal LRCs
- Cyclic and constacyclic LRCs

Some interesting problems and related research topics will also be discussed, which are given as follows:

- Improving the upper bounds for the code length of Singleton-optimal LRCs and providing new constructions of LRCs (asymptotically) achieving these bounds.
- Finding perfect LRCs with new parameters, and even determining all possible perfect LRCs, just like classical perfect LRCs

- Finding new (consta)cyclic Singleton-optimal LRCs with code length $n > q + 1$ and new (consta)cyclic perfect LRCs.
- Investigating the array codes with locality and designing efficient encoding/decoding algorithms.

Bibliography

[1] C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, and S. Yekhanin, "Erasure coding in windows azure storage," in *Proc. USENIX Annu. Tech. Conf.*, Boston, MA, USA, pp. 15–26, 2012.

[2] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, "On the locality of codeword symbols," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6925–6934, Nov. 2012.

[3] Prakash N., Kamath G.M., Lalitha V., Kumar P.V., "Optimal linear codes with a local-error-correction property," In: Proc. Int. Symp. Inf. Theory (ISIT), 2776-2780. 2012.

[4] S. Goparaju and R. Calderbank, "Binary cyclic codes that are locally repairable," in *Proc. Int. Symp. Inf. Theory (ISIT)*, Honolulu, HI, USA, pp. 676–680, Jul. 2014.

[5] N. Prakash, G. M. Kamath, V. Lalitha, and P. V. Kumar, "Codes with local regeneration and erasure correction," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4637-4660, Aug. 2014.

[6] Song W., Day S., Yuen C., Li T., "Optimal locally repairable linear codes," *IEEE J. Selected Areas Comm.* **32**, 6925-6934, 2014.

[7] I. Tamo and A. Barg, "A family of optimal locally recoverable codes," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4661-4676, Aug. 2014.

[8] Cadambe V.R., Mazumdar A., "Bounds on the size of locally recoverable codes," *IEEE Trans. Inf. Theory* **61**(11), 5787-5794 2015.

[9] Tamo I., Papailiopoulos D. S., Dimakis A.G., "Optimal locally repairable codes and connections to matroid theory," *IEEE Trans. Inf. Theory* **62**(12), 6661-6671, 2016.

[10] Agarwal A., Barg A., Hu S., Mazumdar A., Tamo I., "Combinatorial alphabet-dependent bounds for locally recoverable codes," *IEEE Trans. Inf. Theory* **64**(5), 3481-3492, 2018.

[11] B. Chen, S. -T. Xia, J. Hao and F. -W. Fu, "Constructions of optimal cyclic (r, δ) locally repairable codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 4, pp. 2499–2511, Apr. 2018.

[12] B. Chen, W. Fang, S. -T. Xia, and F. -W. Fu, "Constructions of optimal (r, δ) locally repairable codes via constacyclic Codes," *IEEE Trans. Communications*, vol. 67, no. 8, pp. 5253–5263, Aug. 2019.

[13] X. Li, L. Ma, and C. Xing, "Optimal locally repairable codes via elliptic curves," *IEEE Trans. Inf. Theory*, vol. 65, no. 1, pp. 108-117, Jan. 2019.

[14] Y. Luo, C. Xing, and C. Yuan, "Optimal locally repairable codes of distance 3 and 4 via cyclic codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 2, pp. 1048–1053, Feb. 2019.

[15] V. Guruswami, C. Xing, and C. Yuan. "How long can optimal locally repairable codes be ?" *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3662–3670, Jun. 2019.

[16] L. Jin, "Explicit construction of optimal locally recoverable codes of distance 5 and 6 via binary constant weight codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 4658–4663, Aug. 2019.

[17] W. Fang and F.-W. Fu, "Optimal cyclic (r, δ) locally repairable codes with unbounded length," *Finite Fields Appli.*, vol. 63, Art. 101650, Mar. 2020.

[18] Hao J., Xia S.-T., Shum K.W., Chen B., Fu F.-W., Yang Y., "Bounds and constructions of locally repairable codes: Parity-check matrix approach," *IEEE Trans. Inf. Theory*, **66**(12), 7465-7474, 2020.

[19] H. Cai, Y. Miao, M. Schwartz, X. Tang, "On optimal locally repairable codes with super-linear length," *IEEE Trans. Inf. Theory*, vol. 66, no. 8, pp. 4853-4868, Mar. 2020.

[20] Chen B., Fang W., Xia S.-T., Hao J., Fu F.-W., "Improved bounds and Singleton-optimal constructions of locally repairable codes with minimum distance 5 and 6," *IEEE Trans. Inf. Theory*, **67**(1), 217-231, 2021.

[21] C. Xing and C. Yuan, "Construction of (r, δ) locally recoverable codes and connection with graph theory," *IEEE Trans. Inf. Theory*, vol. 68, no. 7, pp. 4320 - 4328, Jul. 2022.

[22] G. Luo and S. Ling, “Application of optimal p-ary linear codes to alphabet-optimal locally repairable codes,” *Des. Codes Cryptogr.*, vol. 90, no. 5, pp. 1271–1287, 2022.

[23] W. Fang, B. Chen, S.-T. Xia, F.-W. Fu and X. Chen, “Perfect LRCs and k-optimal LRCs," *Des. Codes Cryptogr.*, vol. 91, pp. 1209–1232, 2023.

[24] W. Fang, F.-W. Fu, B. Chen, and S.-T. Xia, “Singleton-optimal LRCs and perfect LRCs via cyclic and constacyclic codes," *Finite Fields Appli.*, 2023.

[25] G. Luo, M. F. Ezerman, and S. Ling, “Three new constructions of optimal locally repairable codes from matrix-product codes,” *IEEE Trans. Inf. Theory*, vol. 69, no. 1, pp. 75–85, 2023.

Talk 3: An Introduction to Algebraic Geometry Codes and Related Topics

Liming Ma

School of Mathematical Sciences,
University of Science and Technology of China, Hefei 230026, China
lmma20@ustc.edu.cn

Biography
Liming Ma received his Ph.D. degree in mathematics from Nanyang Technological University, Singapore, in 2014. From April 2014 to May 2020, he was a Lecturer with the School of Mathematical Sciences, Yangzhou University, China. Since June 2020, he has been a research associate professor in the School of Mathematical Sciences, University of Science and Technology of China. He is interested in algebraic function fields over finite fields and coding theory, in particular rational places and automorphism groups of algebraic function fields, locally repairable codes, algebraic geometry codes and sequences. He has published more than 10 articles on the journal of Trans. Amer. Math. Soc., IEEE Trans. Inf. Theory, IEEE Trans. Commun., J. Combin. Theory Ser. A, and J. Number Theory.

Abstract
Around 1980, Goppa introduced a new family of blocks codes by using algebraic curves with many rational points over finite fields. The discovery of algebraic geometry codes led to asymptotically good sequences of codes which exceeds the famous Gilbert-Varshamov bound, which was a classical benchmark for families of good linear codes. Algebraic geometry codes are one of the most important family of block codes and have many applications in both coding theory and cryptography. As a natural generalization of the Reed-Solomon codes, algebraic geometry codes have large lengths compared to the alphabet size. However, there are no fast encoding and decoding algorithms for algebraic geometry codes, compared with the Reed-Solomon codes.

After the invention of algebraic geometry codes, algebraic curves over finite fields have attracted many researchers from coding theory, not only algebraic geometry or number theory. Constructing new maximal curves or towers of function fields achieving the Drinfeld-Vladut bound are close related mathematical topics of algebraic geometry codes. Algebraic geometry codes or algebraic curves over finite fields have many applications in coding theory and cryptography, such as locally repairable codes, quantum codes, secret sharing, multiparty computations and sequences, etc.

Our talk will introduce the research progresses in this area, including the following topics:

- an overview of previously known results on algebraic geometry codes,
- various constructions of algebraic geometry codes with good parameters, and asymptotically good sequences of algebraic geometry codes exceeding the Gilbert-Varshamov bound or Tafasman-Valdut-Zink bound,
- optimal and asymptotically good locally repairable codes via subcodes of algebraic geometry codes.

Open problems and some related research topics will also be discussed, which are given as fol-

lows:

- finding maximal curves or curves with many rational points over finite fields and studying their properties, such as GK curves, BM curves, etc.
- determining the Ihara's constant $A(q)$.
- fast encoding of algebraic geometry codes, including algebraic geometry codes exceeding the Gilbert-Varshamov bound or Tafasman-Valdut-Zink bound.
- fast decoding of algebraic geometry codes, including unique decoding and list decoding.
- finding other applications of algebraic geometry codes in cryptography and coding theory.

Bibliography

[1] A. Barg, I. Tamo, and S. Vlăduţ, *Locally recoverable codes on algebraic curves*, IEEE Trans. Inf. Theory, vol. 63, no. 8, pp. 4928–4939, Aug. 2017.

[2] A. Bassa, P. Beelen, A. Garcia and H. Stichtenoth, *Towers of function fields over non-prime finite fields*, Mosc. Math. J., vol. 15, pp. 1–29, 2015.

[3] P. Beelen and M. Montanucci, *A new family of maximal curves*, J. London Math. Soc., vol. 98, no. 2, pp. 573–592, 2018.

[4] P. Beelen, J. Rosenkilde and G. Solomatov, *Fast encoding of AG codes over C_{ab} curves*, IEEE Trans. Inf. Theory, vol. 67, no. 3, pp. 161–1655, Mar. 2020.

[5] P. Beelen, J. Rosenkilde and G. Solomatov, *Fast decoding of AG codes*, IEEE Trans. Inf. Theory, vol. 68, no. 11, pp. 7215–7232, Nov. 2022.

[6] N. Elkies, *Excellent nonlinear codes from modular curves*, in STOC'01, Proc. 33rd Annu. ACM Symp. Theory of Computing, Hersonissos, Crete, Greece, pp. 200-208, 2001.

[7] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound*, Invent. Math., vol. 121, pp. 211–222, 1995.

[8] A. Garcia and H. Stichtenoth, *On the asymptotic behavior of some towers of function fields over finite fields*, J. Number Theory, vol. 61, no.2, pp. 248–273, 1996.

[9] M. Giulietti and G. Korchmaros, *A new family of maximal curves over a finite field*, Math. Ann., vol. 343, pp. 229–245, 2009.

[10] V. Guruswami and C. Xing, *Optimal rate list decoding over bounded alphabets using algebraic geometry codes*, J. ACM, vol. 69, no. 2, pp. 1–48, 2022.

[11] X. Li, L. Ma and C. Xing, *Optimal locally repairable codes via elliptic curves*, IEEE Trans. Inf. Theory **65**(2019), no. 1, 108–117.

[12] X. Li, L. Ma and C. Xing, *Construction of asymptotically good locally repairable codes via automorphism groups of function fields*, IEEE Trans. Inf. Theory **65**(2019), no. 11, 7087–7094.

[13] S. Liu, T. Wu and C. Xing, *Nonlinear codes exceeding the Gilbert-Varshmov and Tsfasman-Vladut-Zink bound*, SODA, pp. 4104–4114, 2022.

[14] L. Jin, L. Ma and C. Xing, *Construction of optimal locally repairable codes via automorphism groups of rational function fields*, IEEE Trans. Inf. Theory **66**(2020), no. 1, 210–221.

[15] L. Jin, L. Ma and C. Xing, *A new construction of nonlinear codes via rational function fields*, IEEE Trans. Inf. Theory, vol. 67, no. 2, pp. 770–777, Feb. 2021.

[16] L. Jin, L. Ma and C. Xing, *Binary sequences with a low correlation via cyclotomic function fields*, IEEE Trans. Inf. Theory, vol. 68, no. 5, pp. 3445–3454, May 2022.

[17] L. Ma and C. Xing, *Constructive asymptotic bounds of locally repairable codes via function fields*, IEEE Trans. Inf. Theory **66**(2020), no. 9, 5395–5403.

[18] H. Stichtenoth and C. Xing, *Excellent nonlinear codes from algebraic function fields*, IEEE Trans. Inf. Theory, vol. 51, no. 11, pp. 4044–4046, Nov. 2005.

[19] I. Tamo and A. Barg, *A family of optimal locally recoverable codes*, IEEE Trans. Inf. Theory **60**(2014), no.8, 4661–4676.

[20] M.A. Tsfasman, S.G. Vladut and T. Zink, *Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound*, Math. Nachr., vol. 109, pp. 21–28, 1982.