Curriculum Vitae

Qi Cheng

School of Computer Science
The University of Oklahoma
Norman, OK 73019

Email: qcheng@ou.edu
Phone: (405)325-1017
Fax: (405)325-4044

RESEARCH INTERESTS

- Cryptography, Computational Number Theory, Coding Theory, and Computational Complexity.
- Algorithmic Self-Assembly and DNA Computing.

EDUCATION

- Ph.D. in Computer Science, University of Southern California, 2001.
- M.Sc. in Computer Science, Fudan University, China, 1995.
- B.Sc. in Computer Science, Nankai University, China, 1992.

PROFESSIONAL EXPERIENCE

- Professor, School of Computer Science, University of Oklahoma, July 2014 —
- Associate Professor, School of Computer Science, University of Oklahoma, Aug. 2007 — June 2014.
- Assistant Professor, School of Computer Science, University of Oklahoma, Aug. 2001— June 2007.
- Research Assistant, University of Southern California, Aug. 1997—Aug. 2001.
- Teaching Assistant, University of Southern California, Aug. 1997—May 1999.
- Research Assistant, University of California, Riverside, Sept. 1996—May 1997.
- Assistant Lecturer, Fudan University, Aug. 1995—Jul. 1996.

AWARDS and GRANTS

- Principle Investigator. AF: Medium: Collaborative Research: Arithmetic Geometry Methods in Complexity and Communication, NSF CCF-1900820. 2019–2022. $282740.
- Professor of the Year, School of Computer Science, University of Oklahoma, 2017.
- Principle Investigator. AF: Medium: Collaborative Research: Sparse Polynomials, Complexity, and Algorithms, NSF grant CCF-1409294. 2014–2017. $223168.
- Williams Companies Foundation Presidential Professor, July 2014 —

- Distinguished Paper Award. The International Symposium on Symbolic and Algebraic Computation (ISSAC) 2013, presented by Association for Computing Machinery (ACM) Special Interest Group on Symbolic and Algebraic Manipulation.
- Principle Investigator. Zero Testing and Sign Determination of Algebraic Numbers, NSF grant CCF-0830522. 2009–2012. $198491.
- Principle Investigator. Collaborative Research: Complexity and Algorithms of Decoding Algebraic Codes, NSF grant CCF-0830522. 2009–2012. $197592.
- Principle Investigator. Research in Algorithmic Theory of Self-Assembly. NSF CAREER Award CCR-0237845, 2003–2008. $400,000.
- Dean F. Hougen, Qi Cheng, Amy McGovern, Yifei Dong, and Andrew Fagg. Computer Science Graduate Fellowship Program, Graduate College and College of Engineering, University of Oklahoma. $230,000. August 2006-May 2015.
- University of Oklahoma Junior Faculty Research Award, 2002. $6,000.
- American Institute of Mathematics Travel Grant, 2003, 2006.
- STOC Student Travel Award, 2001.
- Fudan University Motorola Fellowship, 1994.

JOURNAL PUBLICATIONS

[1] Jincheng Zhuang, Qi Cheng, and Jiejing Wen. "Solution Counts and Sums of Roots of Unity". In: *Journal of Number Theory* 240 (Nov. 2022), pp. 551–561.

[2] Qi Cheng, J. Maurice Rojas, and Daqing Wan. "Computing zeta functions of large polynomial systems over finite fields". In: *J. Complexity* 73 (2022), p. 101681. DOI: 10.1016/j.jco.2022.101681. URL: https://doi.org/10.1016/j.jco.2022.101681.

[3] Qi Cheng, Jun Zhang, and Jincheng Zhuang. "LWE from non-commutative group rings". In: *Designs, Codes and Cryptography* 90.1 (2022), pp. 239–263. DOI: 10.1007/s10623-021-00973-6. URL: https://doi.org/10.1007/s10623-021-00973-6.

[4] Dianyan Xiao and Qi Cheng. "A faster method to compute primitive elements and discrete logarithms of factor base in Artin-Schreier extensions". In: *Sci China Inf Sci* 62.9 (2019).

[5] Dianyan Xiao, Jincheng Zhuang, and Qi Cheng. "Factor base discrete logarithms in Kummer extensions". In: *Finite Fields and Applications* 53 (2018), pp. 205–225.

[6] Qi Cheng, Shuhong Gao, J. Maurice Rojas, and Daqing Wan. "Sparse univariate polynomials with many roots over finite fields". In: *Finite Fields and Their Applications* 46 (2017), pp. 235–246.

[7] Jingguo Bi, Qi Cheng, and J. Maurice Rojas. "Sub-linear Root Detection, and New Hardness Results, for Sparse Polynomials Over Finite Fields". In: *SIAM journal on Computing* 45.4 (2016), pp. 1433–1447.

[8] Jincheng Zhuang, Qi Cheng, and Jiyou Li. "On Determining Deep Holes of Generalized Reed-Solomon Codes". In: *IEEE Transactions On Information Theory* 62.1 (2016), pp. 199–207.

[9] Jingguo Bi and Qi Cheng. "Lower Bounds of Shortest Vector Lengths in Random NTRU Lattices". In: *Theoretical Computer Science* 560 (2014), pp. 121–130.

[10] Qi Cheng, Daqing Wan, and Jincheng Zhuang. "Traps to the BGJT-Algorithm for Discrete Logarithms". In: *LMS Journal of Computation and Mathematics* 17 (2014). Special Issue for ANTS-XI, DOI: 10.1112 / S1461157014000242, pp. 218–229.

[11] Qi Cheng and Jincheng Zhuang. "On certain computations of Pisot numbers". In: *Information Processing Letters* 113 (2013), pp. 271–275.

[12] Qi Cheng and Daqing Wan. "A Deterministic Reduction for the Gap Minimum Distance Problem". In: *IEEE Transactions on Information Theory* 58.11 (2012). DOI: 10.1109 / TIT.2012.2209198, pp. 6935–6941.

[13] Qi Cheng and Yu-Hsin Li. "On the minimum gap between sums of square roots of small integers". In: *Theoretical Computer Science* 412 (2011), pp. 5458–5465.

[14] Qi Cheng and Daqing Wan. "Complexity of Decoding Positive-Rate Primitive Reed-Solomon Codes". In: *IEEE Transactions on Information Theory* 56.10 (2010). DOI: 10.1109 / TIT.2010.2060234, pp. 5217–5222.

[15] Qi Cheng, Xianmeng Meng, Celi Sun, and Jiazhe Chen. "Bounding the sum of square roots via lattice reduction". In: *Mathematics of Computation* 79.270 (2010), pp. 1109–1122.

[16] Qi Cheng, Sergey P. Tarasov, and Mikhail N. Vyalyi. "Efficient Algorithms for Sparse Cyclotomic Integer Zero Testing". In: *Theory of Computing Systems* 46.1 (2010), pp. 120–142.

[17] Qi Cheng. "Hard problems of Algebraic Geometry codes". In: *IEEE Transactions on Information Theory* 54.1 (2008). DOI: 10.1109 / TIT.2007.911213, pp. 402–406.

[18] Qi Cheng. "Constructing finite field extensions with large order elements". In: *SIAM journal on Discrete Mathematics* 21.3 (2007), pp. 726–730.

[19] Qi Cheng. "Primality Proving via One Round in ECPP and One Iteration in AKS". In: *Journal of Cryptology* 20.3 (2007), pp. 375–387.

[20] Qi Cheng and Daqing Wan. "On the List and Bounded Distance Decodability of Reed-Solomon Codes". In: *SIAM Journal on Computing* 37.1 (2007). Special Issue on FOCS 2004. DOI: 10.1137 / S0097539705447335, pp. 195–209.

[21] Qi Cheng and Ming-Deh Huang. "On Partial Lifting and the Elliptic Curve Discrete Logarithm Problem". In: *Algorithmica* 46.1 (2006), pp. 59–68.

[22] Qi Cheng. "On the Bounded Sum-of-digits Discrete Logarithm Problem in Finite Fields". In: *SIAM Journal on Computing* 34.6 (2005), pp. 1432–1442.

[23] Qi Cheng. "On the construction of finite field elements of large order". In: *Finite Fields and Their Applications* 11.3 (2005). DOI: 10.1016 / j.ffa.2005.06.001, pp. 358–366.

[24] Gagan Aggarwal, Qi Cheng, Michael H. Goldwasser, Ming-Yang Kao, Pablo Moisset de Espanes, and Robert T. Schweller. "Complexities for Generalized Models of Self-Assembly". In: *SIAM Journal on Computing* 34.6 (2005). DOI: 10.1137 / S00975-39704445202, pp. 1493–1515.

[25] Qi Cheng. "On the Ultimate Complexity of Factorials". In: *Theoretical Computer Science* 326.1-3 (2004), pp. 419–429.

[26] Qi Cheng. "Straight Line Programs and Torsion Points on Elliptic Curves". In: *Computational Complexity* 12.3-4 (2003), pp. 150–161.

[27] Qi Cheng and Ming-Deh Huang. "On counting and generating curves over small finite fields". In: *Journal of Complexity* 20.2–3 (2004).

[28] Qi Cheng and Fang Fang. "Kolmogorov random graphs only have trivial stable colorings". In: *Information Processing Letters* 81.3 (2002), pp. 133–136.

[29] Q. Cheng, M. Chrobak, and G. Sundaram. "Computing Simple Paths among Obstacles". In: *Computational Geometry: Theory and Applications* 16 (2000), pp. 223–233.

[30] Qi Cheng and Hong Zhu. "MNP: a class of NP optimization problems". In: *J. Comput. Sci. Tech.* 12.4 (1997), pp. 306–313.

REFEREED CONFERENCE PUBLICATIONS

[1] Yanbin Pan, Jun Xu, Nick Wadleigh, and Qi Cheng. "On the ideal shortest vector problem over random rational primes". In: *Advances in Cryptology–EUROCRYPT*. Springer-Verlag, 2021. DOI: 10.1007/978-3-030-77870-5_20.

[2] Qi Cheng, Shuhong Gao, J. Maurice Rojas, and Daqing Wan. "Counting roots for polynomials modulo prime powers". In: *Proceedings of Thirteenth Algorithmic Number Theory Symposium ANTS-XIII*. Open Book Series. Mathematical Sciences Publishers, 2018.

[3] Jincheng Zhuang and Qi Cheng. "Generating Coset Representatives of $PGL_2(\mathbf{F}_q)$ in $PGL_2(\mathbf{F}_{q^2})$". In: *11th International Conference on Information Security and Cryptology (Inscrypt)*. 2015.

[4] Qi Cheng, Shuhong Gao, J. Maurice Rojas, and Daqing Wan. "Sparse Univariate Polynomials with Many Roots Over a Finite Field". In: *The Thirteenth Conference on Effective Methods in Algebraic Geometry (MEGA)*. University of Trento, Italy. 2015.

[5] Qi Cheng, Jincheng Zhuang, and Jiyou Li. "On Determining Deep Holes of Generalized Reed-Solomon Codes". In: *Proceedings of The 24th International Symposium on Algorithms and Computation (ISAAC)*. Hong Kong, China, 2013.

[6] Jingguo Bi, Qi Cheng, and J. Maurice Rojas. "Sub-linear Root Detection, and New Hardness Results, for Sparse Polynomials Over Finite Fields". In: *Proceedings of International Symposium on Symbolic and Algebraic Computation (ISSAC)*. DOI: 10.1145 / 2465506.2465514. Boston, MA: ACM press, 2013.

[7] Qi Cheng, Joshua E. Hill, and Daqing Wan. "Counting Value Sets: Algorithm and Complexity". In: *Tenth Algorithmic Number Theory Symposium (ANTS-X)*. DOI: 10.2140 / obs.2013.1.235. 2012.

[8] Jingguo Bi and Qi Cheng. "Lower Bounds of Shortest Vector Lengths in Random NTRU Lattices". In: *The 9th annual conference on Theory and Applications of Models of Computation (TAMC)*. Vol. 7287. Lecture Notes in Computer Science. Springer-Verlag, 2012.

[9] Qi Cheng, Shuhong Gao, and Daqing Wan. "Constructing high order elements through subspace polynomials". In: *Proceedings of the Twenty-Third Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. 2012, pp. 1457–1463.

[10] Qi Cheng and Yu-Hsin Li. "Finding the smallest gap between sums of square roots". In: *Proceedings of The 9th Latin American Theoretical Informatics Symposium (LATIN)*. Vol. 6034. Lecture Notes in Computer Science. 2010, pp. 446–455.

[11] Qi Cheng and Daqing Wan. "A Deterministic Reduction for the Gap Minimum Distance Problem". In: *Proceedings of the 41st ACM Symposium on Theory of Computing (STOC)*. 2009, pp. 33–38.

[12] Qi Cheng and Daqing Wan. "Complexity of Decoding Positive-Rate Reed-Solomon Codes". In: *Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP)*. Vol. 5125. Lecture Notes in Computer Science. Springer-Verlag, 2008.

[13] Qi Cheng. "Derandomization of Sparse Cyclotomic Integer Zero Testing". In: *Proc. 48th IEEE Symp. on Foundations of Comp. Science (FOCS)*. 2007, pp. 74–80.

[14] Qi Cheng and Elizabeth Murray. "On Deciding Deep Holes of Reed-Solomon Codes". In: *Proceedings of Annual Conference on Theory and Applications of Models of Computation(TAMC)*. Vol. 4484. Lecture Notes in Computer Science. Springer-Verlag, 2007, pp. 296–305.

[15] Qi Cheng. "On comparing sums of square roots of small integers". In: *Proc. of 31st International Symposium on Mathematical Foundations of Computer Science (MFCS)*. Vol. 4162. Lecture Notes in Computer Science. 2006.

[16] Qi Cheng and Ming-Deh Huang. "On Partial Lifting and the Elliptic Curve Discrete Logarithm Problem". In: *Proceeding of the 15th Annual International Symposium on Algorithms and Computation (ISAAC)*. Vol. 3341. Lecture Notes in Computer Science. Springer-Verlag, 2004, pp. 342–351.

[17] Qi Cheng and Daqing Wan. "On the List and Bounded Distance Decodibility of the Reed-Solomon Codes (Extended Abstract) (FOCS)". In: *Proc. 45th IEEE Symp. on Foundations of Comp. Science*. 2004, pp. 335–341.

[18] Qi Cheng. "On the Bounded Sum-of-digits Discrete Logarithm Problem in Finite Fields". In: *Proc. of the 24th Annual International Cryptology Conference (CRYPTO)*. Springer-Verlag, 2004, pp. 201–212.

[19] Q. Cheng, A. Goel, and P. Moisset. "Optimal self-assembly of counters at temperature two". In: *The proceedings of the first conference on Foundations of nanoscience: self-assembled architectures and devices*. Invited paper. 2004.

[20] L. Adleman, Q. Cheng, A. Goel, M. Huang, and H. Wasserman. "Linear Self-Assemblies: Equilibria, Entropy, and Convergence Rates". In: *New Progress in Difference Equations*. Ed. by S. Elaydi, G. Ladas, and B. Aulbach. Taylor and Francis, 2003.

[21] Qi Cheng. "Constructing finite field extensions with large order elements". In: *ACM-SIAM Symposium on Discrete Algorithms (SODA)*. 2004, pp. 1123–1124.

[22] Ho-Lin Chen, Qi Cheng, Ashish Goel, Ming-Deh Huang, and Pablo Moisset de Espanes. "Invadable Self-Assembly: Combining Robustness with Efficiency". In: *ACM-SIAM Symposium on Discrete Algorithms (SODA)*. 2004.

[23] Qi Cheng. "Primality Proving via One Round in ECPP and One Iteration in AKS". In: *Proc. of the 23rd Annual International Cryptology Conference (CRYPTO)*. Ed. by Dan Boneh. Vol. 2729. Lecture Notes in Computer Science. Santa Barbara: Springer-Verlag, 2003, pp. 338–348.

[24] Qi Cheng. "On the Ultimate Complexity of Factorials". In: *The 20th International Symposium on Theoretical Aspects of Computer Science (STACS)*. Vol. 2607. Lecture Notes in Computer Science. Springer-Verlag, 2003, pp. 157–166.

[25] Qi Cheng. "Some Remarks on the L-conjecture". In: *Proc. of the 13th Annual International Symposium on Algorithms and Computation (ISAAC)*. Vol. 2518. Lecture Notes in Computer Science. Springer-Verlag, 2002.

[26] L. Adleman, Q. Cheng, A. Goel, M. Huang, David Kempe, Pablo Moisset, and Paul Rothemund. "Combinatorial Optimization Problems in Self-Assembly". In: *Proc. 34th ACM Symp. on Theory of Computing (STOC)*. 2002.

[27] Qi Cheng and Shigenori Uchiyama. "Nonuniform polynomial time algorithm to solve decisional Diffie-Hellman problem in finite fields under conjecture". In: *Proceeding of RSA Conference 2002 Cryptographers Track (CT_RSA)*. Vol. 2271. Lecture Notes in Computer Science. Springer-Verlag, 2002.

[28] L. Adleman, Q. Cheng, A. Goel, and M. Huang. "Running time and program size for self-assembled squares". In: *Proc. 33th ACM Symp. on Theory of Computing (STOC)*. DOI: 10.1145 / 380752.380881. 2001.

[29] Qi Cheng and Ming-Deh Huang. "Factoring Polynomials over Finite Fields and Stable Colorings of Tournaments". In: *Proceeding of Algorithmic Number Theory Symposium (ANTS) IV*. Vol. 1838. Lecture Notes in Computer Science. Springer-Verlag, 2000.

[30] Qi Cheng and Hong Zhu. "MNP: A Class of NP Optimization Problems (Extended Abstract)". In: *Proceeding of Annual International Computing and Combinatorics Conference (COCOON)*. Vol. 959. Lecture Notes in Computer Science. Springer-Verlag, 1995, pp. 559–565.

TECHNICAL REPORTS and OTHER PUBLICATIONS

- Qi Cheng, A New Class of Unsafe Primes, Cryptology ePrint Archive, 2002.
- Qi Cheng, Hong Zhu and Jing Wu, On the Connectivity of a n-pancake Networks, *Journal of Computer Research and Development*, 7, 1–5, 1995. (In Chinese)
- Hong Zhu, Jing Wu and Qi Cheng, Enumerating All Primary Polynomials, *Theoretical Computer Science in China*, 2:163–170, 1994.
- Qi Cheng and Hong Zhu, How Difficult is It to Obtain a Chromatic Polynomial? *Proceeding of the International Workshop on Discrete Mathematics and Algorithms*, 172–176, 1994.

COLLOQUIUM and CONFERENCE TALKS

1. *Lattices Theory*, Shandong University virtual seminar, July 2022.
2. *On the ideal shortest vector problem over random rational primes*, Eurocrypt October 2021. Virtual presentation.
3. *Computational Number Theory*, Shandong University virtual seminar, July 2021.
4. *The Discrete Logarithms over Finite Fields*, Shandong University virtual seminar, October 2020.
5. *The Discrete Logarithms over Kummer and Artin-Schreier extensions*, Carleton University finite fields eSeminar, August 2020.
6. *Counting roots for polynomials modulo prime powers*, Qingdao University, 2019.
7. *Counting roots for polynomials modulo prime powers*, Shandong University, Chinese Academy of Sciences, Guangzhou University, Shanghai Jiaotong University and Capital Normal University, 2018.
8. *Counting roots for polynomials modulo prime powers*, Thirteenth Algorithmic Number Theory Symposium ANTS-XIII, Madison, Wisconsin, July 2018.
9. *Counting roots for polynomials modulo prime powers*, Finite fields and their applications, Shijiazhuang, China May 2018
10. *LWE from Non-commutative Group Rings*, Department of Mathematics, University of Colorado, October 2017.
11. *LWE from Non-commutative Group Rings*, AMS Sectional Meeting, Charleston, SC, March 2017.
12. *The Discrete Logarithms and the Algorithms*, The Institute for Theoretical Computer Science (ITCS), Shanghai University of Finance and Economics (SUFE), July 2016.
13. *Survey on the Lattice-based Cryptography*, Finite fields and their applications, Tianjin, China June 2016
14. *Cryptography: From Art to Science*, Network Center, Chinese Academy of Sciences, July 2015.
15. *Factor base Discrete logarithms in Kummer Extensions*, Hubei University, Wuhan, July 2015.

16. *Traps to the BGJT-Algorithm for Discrete Logarithms*, Finite Fields and Their Applications, Beijing, June 2014.
17. *Traps to the BGJT-Algorithm for Discrete Logarithms*, Eleventh Algorithmic Number Theory Symposium ANTS-XI (2014), GyeongJu, Korea, August 6 – 11, 2014.
18. *Sub-Linear Root Detection, and New Hardness Results, for Sparse Polynomials Over Finite Fields*, Dept. of Mathematics, Tsinghua University, Beijing, Dec 2013.
19. *On determining deep holes of Generalized Reed- Solomon codes*, The 24th International Symposium on Algorithms and Computation (ISAAC), Hong Kong, China, Dec. 2013.
20. *Sub-Linear Root Detection, and New Hardness Results, for Sparse Polynomials Over Finite Fields*, International Symposium on Symbolic and Algebraic Computation (ISSAC), Boston, June 2013.
21. *On the Decodability of Primitive Reed-Solomon Codes*, University of Michigan, Ann Arbor, MI, February 2013.
22. *Sub-Linear Root Detection, and New Hardness Results, for Sparse Polynomials Over Finite Fields*, Finite Fields and Their Applications, Beijing, June 2012.
23. *On the Decodability of Primitive Reed-Solomon Codes*, Sichuan University, May, 2012.
24. *Bounding the Sum of Square Roots via Lattice Reduction*, Institute of Software, Chinese Academy of Sciences, July, 2012.
25. *Lower Bounds of Shortest Vector Lengths in Random NTRU Lattices*. The 9th annual conference on Theory and Applications of Models of Computation (TAMC 2012), Beijing. May 2012.
26. *Cryptography: From Art to Science*. The Computing and Technology (CaT) week at Cameron University, April, 2012.
27. *Constructing high order elements through subspace polynomials*. The Number Theory Seminar in University of California, Irvine, March, 2012.
28. *Constructing high order elements through subspace polynomials*. The ACM-SIAM Symposium on Discrete Algorithms (SODA) 2012, Kyoto, Japan.
29. *On the Decodability of Primitive Reed-Solomon Codes*, The SIAM Conference on Applied Algebraic Geometry (AG11), Raleigh, North Carolina, Oct. 2011.
30. *Bounding the Sum of Square Roots via Lattice Reduction*, The SIAM Conference on Applied Algebraic Geometry (AG11), Raleigh, North Carolina, Oct. 2011.
31. *Lower bounds of shortest vector lengths in random NTRU lattices*, Institute of Mathematics, Chinese Academy of Science. July 2011.
32. *Identity Testing and Sign Determination of Algebraic Numbers*, invited talk (45 minutes), International Congress of Chinese Mathematicians 2010, Beijing, China.
33. *Identity Testing and Sign Determination of Algebraic Numbers*, Clemson University, November 2010, Clemson, SC.
34. *Identity Testing and Sign Determination of Algebraic Numbers*, Tsinghua University, July 2010, Beijing, China.

35. *Finding the smallest gap between sums of square roots* , The 9th Latin American Theoretical Informatics Symposium (LATIN) April 2010, Oaxaca, Mexico.

36. *A Deterministic Reduction for the Gap Minimum Distance Problem*, East China Normal University, July 2009, Shanghai, China.

37. *Zero testing and sign determination of straight-line integers*, Fudan University, June 2009, Shanghai, China.

38. *A Deterministic Reduction for the Gap Minimum Distance Problem*, The 41st ACM Symposium on Theory of Computing (STOC), May 2009, Washington DC.

39. *Derandomization of Sparse Cyclotomic Integer Zero Testing*, University of Colorado, Boulder, April 2009.

40. *A Deterministic Reduction for the Gap Minimum Distance Problem*, Rutgers University, Piscataway, NJ, April 2009.

41. *A Number Theoretic Memory Bounded Function and Its Applications*, The 2008 International Symposium on Trusted Computing, Zhangjiajie, China. Nov 2008.

42. *Derandomization of Sparse Cyclotomic Integer Zero Testing*, Nankai University, China. Nov 2008.

43. *Derandomization of Sparse Cyclotomic Integer Zero Testing*, Shandong University, China. Nov 2008.

44. *Complexity of Decoding Positive-Rate Reed-Solomon Codes*, The 35th International Colloquium on Automata, Languages and Programming. Reykjavik, Iceland. July 2008.

45. *Complexity of Decoding Positive-Rate Reed-Solomon Codes*, The 3th Workshop on Finite Fields and Their Applications, Zhenzhou, China. June 2008.

46. *Derandomization of Sparse Cyclotomic Integer Zero Testing*, Microsoft Research Asia Theory Workshop. Beijing, China. April 2008.

47. *Derandomization of Sparse Cyclotomic Integer Zero Testing*, The 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS), Providence, Rhode Island, Oct. 2007.

48. *On comparing sums of square roots of small integers.* Invited Colloquium in Shanghai Jiaotong University, July 4, 2007.

49. *On comparing sums of square roots of small integers.* Center for Advanced Study, Tsinghua University, Beijing, China. June 2007.

50. *On Deciding Deep Holes of Reed-Solomon Codes.* The 4th Annual Conference on Theory and Applications of Models of Computation (TAMC07). Shanghai, China, May 2007.

51. *On Deciding Deep Holes of Reed-Solomon Codes.* Invited Colloquium in East China Normal University, Shanghai, China, May 18, 2007.

52. *On Deciding Deep Holes of Reed-Solomon Codes.* Invited Colloquium in University of California, Irvine, May 10, 2007.

53. *On comparing sums of square roots of small integers.* The 31st International Symposium on Mathematical Foundations of Computer Science. Stara Lesna, Slovakia. August 2006.

54. *On the Construction of Finite Fields Elements of Large Order.* Invited talk. International Workshop on Finite Fields and Their Applications. Beijing, July 2006.

55. *Hard Problems of Algebraic Geometry Codes.* Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC). Las Vegas, February 2006.

56. *An Efficient Keyless Number-Theoretic Hash.* Workshop on Number Theory Inspired by Cryptography, The Banff International Research Station for Mathematical Innovation and Discovery, Canada. November 2005.

57. *Hard Problems of Algebraic Geometry Codes.* Invited Colloquium in University of California, Irvine, June 2005.

58. *On the List and Bounded Distance Decodibility of the Reed-Solomon Codes.* Invited Colloquium in Fudan University, Shanghai, China. January 2005.

59. *On Partial Lifting and the Elliptic Curve Discrete Logarithm Problem.* The 15th International Symposium on Algorithms and Computation (ISAAC 2004), Hong Kong, China. December 2004.

60. *On the List and Bounded Distance Decodibility of the Reed-Solomon Codes.* Workshop on finite fields and applications, Mathematisches Forschungsinstitut Oberwolfach, December 2004.

61. *On the List and Bounded Distance Decodibility of the Reed-Solomon Codes.* The 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2004, Rome, Italy.

62. *On the Bounded Sum-of-digits Discrete Logarithm Problem in Finite Fields.* The 24th Annual International Cryptology Conference (CRYPTO) 2004, Santa Barbara, CA.

63. *On the List and Bounded Distance Decodibility of the Reed-Solomon Codes.* Invited Colloquium in University of California, Irvine, May 2004.

64. *Some Remarks on the L-conjecture.* Number Theory Seminar in University of California, Irvine, May 2004.

65. *Constructing finite field extensions with large order elements.* ACM-SIAM Symposium on Discrete Algorithms (SODA) 2004, New Orleans, LA.

66. *Primality Proving via One Round in ECPP and One Iteration in AKS.* The 23rd Annual International Cryptology Conference (CRYPTO) 2003, Santa Barbara, CA

67. *Primality Proving via One Round in ECPP and One Iteration in AKS.* AIM Workshop on Future Directions in Algorithmic Number Theory, Palo Alto, CA, March 2003.

68. *On the Ultimate Complexity of Factorials.* The 20th International Symposium on Theoretical Aspects of Computer Science (STACS), 2003, Berlin.

69. *Some Remarks on the L-conjecture.* The 13th Annual International Symposium on Algorithms and Computation (ISAAC), 2002, Vancouver, Canada.

70. *Introduction to the AKS Primality Testing.* University of Oklahoma, Norman, OK, Oct 25, 2002.

71. *Nonuniform Polynomial Time Algorithm to Solve Decisional Diffie-Hellman Problem in Finite Fields under Conjecture.* RSA Conference Cryptographers Track (CT_RSA), 2002, San Jose, California.

72. *Running Time and Program Size for Self-assembled Squares.* Oklahoma State University, Stillwater, OK, Sept 27, 2001.

73. *Running Time and Program Size for Self-assembled Squares.* University of Oklahoma, Norman, OK, June 7, 2001.

COURSES INTRODUCED

- Algorithmic Coding Theory, Fall 2005.
- Cryptography, Spring 2002.
- Molecular and Quantum Computing, Fall 2004.
- Computer Security, Fall 2016.

COURSES TAUGHT

- Cryptography, Spring 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2010, 2011, 2012, 2013, 2014, 2015.
- Database, Fall 2006, 2007, 2009, 2010, 2011.
- Programming Language Concepts, Fall 2001, 2002, 2003, Spring 2008, 2010, 2011, 2012, 2013, 2014, 2015.
- Algorithm Analysis, Spring 2004, 2005.
- Network Security, Fall 2012, 2013, 2014.
- Applied Logic, Fall 2013, 2014.

CHAIR OF PHD DISSERTATION COMMITTEE

- Yu-Hsin Li (Spring 2011), Finding Minimum Gaps and Designing Key Derivation Functions.
- Jincheng Zhuang (Spring 2014), Studies on Deep Holes and Discrete Logarithms.

CHAIR OF MASTER THESIS COMMITTEE

- Xuecheng Chen (2016), Study Of Matrices Related To Discrete Logarithm In Kummer Extensions.
- Nha Hoang (2013), Finite Field Elements Of High Order From Subspace Polynomials.

- Matthew Bodenhamer (2007), A multi-Component Interactive Approach to Combating Spam.
- Elizabeth Murray (2006), On Deciding Deep Holes of Reed-Solomon Codes.
- Manish Sharma (2004), Large Degree Polynomial Computation and Primality Proving.
- Kausthubh Vuchi (2004), A Study of the Order of Certain Groups Related to the AKS Primality Testing.

HOSTING VISITING RESEARCHERS AND STUDENTS

Jun Xu (Chinese Academy of Sciences, Oct 2018–Oct 2019), Yanbin Pan (Chinese Academy of Sciences, Sept 2018– Sept 2019), Jun Zhang (Capital Normal University, Dec 2016–Dec 2017), Haifeng Qian (East China Normal University, 2008), Xianmeng Meng (Shandong University of Finance and Economics, 2008), Suntae Hwang (Daejeon University, 2004–2005)

Jingguo Bi (Shandong University, 2011–2012), Dianyan Xiao (Tsinghua University, 2014).

MEMBER OF PHD DISSERTATION COMMITTEE

Shaojian Fu (2005), Muhammad Javed (2009), Zhaowen Xing (2011), TaChun Lin (2011), Loyd Hook IV (2012), Julia Maddox (2012), Catherine Ann Hall (2012), Brian Cremeans (2014), Maryam Nafari (2014), Husnu Narman (2016), Di Wu (2016), Mamta Yadav (2017), Liangzhe Li (2017), Zheng Li (2017), Jordan Wiebe (2019), Michael Nelson (2019), Chenxiao Wang (2021), Yan Liang (2022).

MEMBER OF MASTER THESIS COMMITTEE

Xiang-rong Jiang (2003), Isaac Harley (2004), Chittaranjan Tripathy (2005), Biao Liu (2006), David Johnson (2006), Mahiro Ando (2007), Liangzhe Li (2013), Mikael Perrin (2015), Nathalie Kaligirwa (2015), Adrien Badre (2018), Jeremy Rand (2018), Catherine Ha (2019).

UNDERGRADUATE RESEARCH GUIDANCE

Jeff Starr, UROP award, 2003.

DEPARTMENT, COLLEGE and UNIVERSITY SERVICE

- Member of Committee A, 2013–2014, 2021–2023.
- Chair of Undergraduate Advising Committee, 2012–2014, 2018–2023.
- Member of Undergraduate Advising Committee, 2010–2012.
- Member of Graduate Committee, 2006–2007, 2011–2012.
- Member of Graduate Enrollment Management Committee, 2005–2006.
- Panel member for the Provost Outstanding Dissertation Award, 2006.
- Member of the Undergraduate Committee, 2009–2010, 2018–2019.
- Member of Deans Senior Advisory Committee, 2009–2010.

- Graduate Faculty Panelist for Appeals/Misconduct, 2009–2010.
- OU speakers service, since 2011.
- Member of Campus Tenure Committee, 2016–2017.
- Member of Faculty Senate, 2016–2017.
- Assistant Coach, Programming Competition, 2014–2020.

PROFESSIONAL SERVICE

- Member of the Poster Committee, The International Symposium on Symbolic and Algebraic Computation (ISSAC) 2020.
- Editor, Indian Journal of Discrete Mathematics, from 2019
- Member of the Program Committee: The 6th Annual International Conference on Combinatorial Optimization and Applications (COCOA 2012, Banff, Canada).
- Member of the Program Committee: The 17th Annual International Computing and Combinatorics Conference (COCOON 2011, Dallas, TX).
- Editorial board, International Journal of Computer Mathematics from 2009 to 2011.
- Participated in NSF CISE Theory Of Computing review panel, 2003, 2004, 2005, 2016.
- Reviewed journal papers for Information Processing Letters (2002), Journal of Computer Science and Technology (2002, 2005), Computational Complexity (2004), Design, Codes and Cryptography (2004, 2008, 2011), SIAM Journal on Computing (2004, 2007, 2008, 2010, 2017, 2018), Applied Mathematics Letters (2004), Discrete Mathematics (2006), IEEE Transaction on Information Theory (2007, 2011, 2015, 2016, 2018, 2021, 2022), Finite Fields and Their Applications (2007, 2009, 2010, 2015, 2016, 2017), Algorithmica (2007), The American Mathematical Monthly (2011), Journal of Mathematical Cryptology (2011), Theory of Computing (2011), ACM Transactions on Computation Theory (2011), Theoretical Computer Science (2014), Mathematics of Computation (2016, 2018), Information and Computation (2016).
- Reviewed conference papers for SODA 2002, 2011, 2014, 2021, ANTS 2004, 2006, 2016, 2020 SCN 2004, ICALP 2005, 2016, STOC 2007, 2012, DNA 2009, FOCS 2005, 2009, 2011, 2020.
- Session chair for TAMC 2007.
- Guest Associate Editor, Japan Journal of Industrial and Applied Mathematics (JJIAM), Special Issue on "Algorithmic Number Theory and Its Applications", 2006.
- A reviewer for American Mathematical Society Mathematical Reviews since 2005.
- Reviewed a proposal for U.S. Civilian Research & Development Foundation (CRDF), 2002.
- Reviewed *Programming Languages: Principles and Paradigms* by Tucker and Noonan, McGraw-Hill.

PUBLIC SPEAKER

1. *Cryptography: From Art to Science*, OU Organizational Staff Council, Nov. 2011.
2. *Cryptography: From Art to Science*, Oklahoma National Guard, May 2014.