Xukai Zou's Curriculum Vitae

Computer Science Department, Indiana University Purdue University Indianapolis
723 W. Michigan ST. SL280, Indianapolis, IN 46202
Web: cs.iupui.edu/∼xzou/; Email: xkzou@cs.iupui.edu

1 Education

- Postdoctoral Fellow: University of Nebraska-Lincoln, 07/2002 - 07/2003.
- PhD in Computer Science, University of Nebraska-Lincoln, 12/2000, GPA: 4.0/4.0.
- MS in Computer Science, Huazhong University of Science and Technology, China, 06/1986, GPA: 4.0/4.0.
- BS in Computer Science, Zhengzhou University, China, 07/1983, GPA: 4.0/4.0.

2 Academic appointments

- *July, 2020 -* : Professor
  Department of Computer and Information Science, Indiana University-Purdue University Indianapolis, IN, USA.
- *July. 2009 - June, 2020*: Associate Professor
  Department of Computer and Information Science, Indiana University-Purdue University Indianapolis, IN, USA.
- *Aug. 2003 - June. 2009*: Assistant Professor
  Department of Computer and Information Science, Indiana University-Purdue University Indianapolis, IN, USA.
- *Oct. 1993 - Dec. 1997*: Associate Professor
  Computer Science Department, Zhengzhou University, Zhengzhou, Henan, China.
- *Jul. 1986 - Sep. 1993*: Lecturer/Assistant Professor
  Computer Science Department, Zhengzhou University, Zhengzhou, Henan, China.

Other Appointments

- *Jan. 2001 - Jun. 2002*: Software Architect
  ACE Information Resource Inc., Fort Lee, NJ, USA.
- *Jan. 1998 - Dec. 2000*: Graduate Teaching/Research Assistant
  Dept. of Computer Science and Engineering, University of Nebraska-Lincoln, NE, USA.

3 Research interests: Cryptography, Cybersecurity, Networking, Deep Learning, and Design & Analysis of Algorithms & Protocols

Recent works: User authentication (biometric & mobile authentication), Secure digital provenance/blockchain technology, Cryptography-based access control, Group key management, Secret sharing, Secure multi-party computation, Moving target defense, Security in mobile, social networks and delay-tolerant networks, Secure electronic voting, Personal health and genomic data security and privacy, combination of security/privacy and deep learning.

4 Grants

(a) External

1. NSF DGE-2146359, *CyberCorps Scholarship for Service: Building the Next Generation Cybersecurity Engineering Workforce*, 2/1/2022–1/31/2027, NSF, $3,729,000, Co-PI (with PI: F. Li and Co-PIs: B. King and D. Russomanno).

2. (Education Research) NSF DGE-2011117, SaTC: EDU: Collaborative: *Building an Electronic Voting Technology Inspired Interactive Teaching and Learning Framework for Cybersecurity Education*, National Science Foundation, 5/1/2021–4/30/2024, $400,000, Lead PI .

3. (REU Supplement) NSF DGE-2011117, SaTC: EDU: Collaborative: *Building an Electronic Voting Technology Inspired Interactive Teaching and Learning Framework for Cybersecurity Education*, National Science Foundation, 8/1/2021–7/31/2022, $16,000, Lead PI .

4. (EDU supplement) NSF DGE-2337533, *CyberSecurity and Cyber Patriot Summer Camp*, June, 2024, $45,999., PI.

5. NSF CICI-1839746, *Development of a Secure and Privacy-Preserving Workflow Architecture for Dynamic Data Sharing in Scientific Infrastructures*, 9/1/2018–12/31/2022, $599,998, PI (with Co-PIs: H. Wu and S. Purkayastha).

6. NSF CNS-1852105, *REU Site: Enhancing Undergraduate Experiences in Mobile Cloud and Data Security*, 12/15/2018 – 11/30/2022, $381,000, Co-PI (with PI: F. Li and Co-PI: X. Luo).

7. NSF CNS-1560020, *REU Site: Enhancing Undergraduate Experience in Mobile Computing Security*, 6/1/2016–5/31/2019, $395,000, Co-PI (with PI: F. Li and E. Fernandez).

8. NSF CNS-1262984, *REU Site: Enhancing Undergraduate Experience in Mobile Computing Security*, 6/1/2013–5/31/2016, $359,964, Co-PI (with PI: F. Li and Co-PI: E. Fernandez).

9. Northrop Grumman, *MovingCloud: Create Moving-target Defense in Cloud by Learning from Botnets*, 10/1/2012–9/31/2013, $107,000 Co-PI (with PI: F. Li)

10. CISCO, *Building A Secure Video Streaming Framework for Dynamic and Anonymous Subscriber Groups*, 07/15/08 – 07/15/09. $85,000, PI.

11. NSF CCR-0311577, *Secure Group Communications over Wired/Wireless Networks*, 08/01/03 - 07/31/07, $349,990, PI (at IUPUI, with PI at UNL: B. Ramamurthy and Co-PI at UNL: V. Variyam).

12. Department of Veterans Affairs, *Secure and Reliable Medical Information Systems*, 01/01/06 - 12/31/07, $156,000, PI (with Co-PI: Y. Dai).

13. IEEE and NASA, *The 2nd IEEE Symposium on Dependable Autonomic and Secure Computing (DASC06)*, 2006, $19,060, Co-PI (with PI: Y. Dai).

(b) Internal

14. IUPUI, 1st Year Research Immersion 1RIP program, *Secure & verifiable online voting.* 9/1/2023 - 8/31/2024, $2,000, PI.

15. IUPUI, iAi, *A Vaccination Framework to Tackle Security Attacks in Horizontal and Vertical Federated Learning Systems*, 6/15/2023 - 6/14/2024, $25,000, Co-PI (with PI: Feng Li).

16. IUPUI, Enhanced Mentoring Program with Opportunities for Ways to Excel in Research (EMPOWER), 4/1/2020 - 3/31/2021, $2,000, PI.

17. IUPUI, Undergraduate Research Opportunities Program (UROP), Mentor award, 2,500 (5*500), 2016-2020, PI.

18. Purdue School of Science Near the Miss grant, *Robust Privacy-preserving Universal Identity and Revocable User-Centric (Active) Authentication Across Cyberspace*, 2016, $26,176, PI.

19. Purdue University Summer Research Grant, *Research and Evaluation of Privacy-Preserving and Replaceable Biometrics-based Authentication*, 2011, $8,000, PI.

20. Indiana University's Center for Applied Cybersecurity Research (CACR) Grant, *Evaluation of Clinical and Genomic Information Privacy Risks from Inference AttackS*, 06/01/10–07/31/11, $49,952, Co-PI (with PI: Jake Chen).

21. Indiana University's Center for Applied Cybersecurity Research (CACR) Grant, *A novel approach to resilient, secure, and cancelable biometrics*, 07/01/09–07/31/10, $33,736, Co-PI (with PI: Yingzi Du and Co-PI: Scott Orr).

22. Purdue University Summer Research Grant, *Implementation and Evaluation of Secure, Composable, and Scalable Framework for Trusted Collaborative Computing*, 2008, $8,000, PI.

23. IUPUI RSFG grant, *Secure and Dependable Medical Information System*, 12/15/05 -12/15/06, $30,000, PI (with Co-PI: Y. Dai).

24. *Signature Center for Bio-Computing*, IUPUI, 2007–2009, $285,000, Co-PI (with PI: Shiaofen Fang and other Co-PIs).

25. *Trusted Collaborative Computing and Robust Group Key Management*, Granted by IU seed fund, 08/01/03 - 06/31/06, $75,000.00, PI.

5 Publications

5.1 Monographs (peer reviewed on the table of contents, introductions, sample chapters)

1. X. Zou, Y. Dai and Y. Pan, *Trust and Security in Collaborative Computing*, World Scientific, ISBN-13: 978-981-270-3682, January 2008, pages 242.

2. X. Zou, B. Ramamurthy and S. Magliveras, *Secure Group Communication over Data Networks*, Springer, ISBN: 0-387-22970-1, October 2004, pages 172.

5.2 Peer-reviewed articles

3. Ryan J Hosler, Agnideven Palanisamy Sundar, Xukai Zou, Feng Li, and Tianchong Gao, *Unsupervised Deep Learning for an Image Based Network Intrusion Detection System*, 2023 IEEE Global Communications Conference: Communication & Information Systems Security, 4–8 December 2023. Kuala Lumpur, Malaysia (Accepted).

4. Niu Zhang, Shunwei Wang, Tianchong Gao , Feng Li, Agnideven Palanisamy Sundar, and Xukai Zou, *Local Differential Privacy Preservation via the Novel Encoding Method*, The 20th IEEE International Conference on Mobile Ad-Hoc and Smart Systems (MASS 2023), Sept. 25 - 27, 2023, Toronto, Canada, (Accepted).

5. Agnideven Palanisamy Sundar, Feng Li, Xukai Zou,Tianchong Gao and Ryan Hosler, *GAN-inspired Defense Against Backdoor Attack on Federated Learning Systems*, The 20th IEEE International Conference on Mobile Ad-Hoc and Smart Systems (MASS 2023), Sept. 25 - 27, 2023, Toronto, Canada, (Accepted).

6. Muwei Zheng, Nathan Swearingen, William Silva, Matt Bishop and Xukai Zou, *An Adaptive Plug-and-Play (PnP) Interactive Platform for an E-Voting based Cybersecurity Curricula.* IFIP International Symposium on Human Aspects of Information Security & Assurance (HAISA'23), 2023, pp. 36-52.

7. Muwei Zheng, Nathan Swearingen, Steven Mills, Croix Gyurek, Matt Bishop and Xukai Zou, *Case Study: Mapping an E-Voting Based Curriculum to CSEC2017*, ACM SIGCSE TS 2023, pp.514-520 **Best Paper Award.**

8. Agnideven Palanisamy Sundar, Feng Li, Xukai Zou and Tianchong Gao, *Distributed Swift and Stealthy Backdoor Attack on Federated Learning*, 16th International Conference on Networking, Architecture, and Storage (NAS 2022), Philadelphia, Oct. 3-4, pp. 1-8, doi: 10.1109/NAS55553.2022.9925353.

9. Qin Hu, Feng Li, Xukai Zou, and Yinhao Xiao, *Solving the Federated Edge Learning Participation Dilemma: A Truthful and Correlated Perspective*, IEEE Transactions on Vehicular Technology, vol. 71, no. 7, pp. 7680-7690, July 2022, doi: 10.1109/TVT.2022.3161099.

10. Ryan Hosler, Tyler Phillips, Xiaoyuan Yu, Agnideven Sundar, Xukai Zou and Feng Li, *Learning Discriminative Features for Adversarial Robustness*, the 17th International Conference on Mobility, Sensing and Networking (MSN 2021), December 13-15, 2021, Virtual, pp. 303-310, doi: 10.1109/MSN53354.2021.00055..

11. Nathan Swearingen, Ryan Hosler and Xukai Zou, *Hardware Speculation Vulnerabilities and Mitigations*, The Fourth International Workshop on Smart Living with IoT, Cloud, and Edge Computing (SLICE 2021) in conjunction with The 18th International Conference on Mobile Ad-Hoc and Smart Systems (MASS - 2021), Oct. 4-7, Virtual, pp. 609-614, doi: 10.1109/MASS52906.2021.00087.

12. Ryan Hosler, Xukai Zou and Matt Bishop, *Electronic Voting Technology Inspired Interactive Teaching and Learning Pedagogy and Curriculum Development for Cybersecurity Education*, In: Drevin L., Miloslavskaya N., Leung W.S., von Solms S. (eds) Information Security Education for Cyber Resilience. WISE 2021. IFIP Advances in Information and Communication Technology, vol 615. pp. 27-43, Springer, Cham. https://doi.org/10.1007/978-3-030-80865-5_3.

13. Saptarshi Purkayastha and Shreya Goyal and B. Oluwala and Tyler Phillips and Huanmei Wu and Xukai Zou, *Usability and Security of Different Authentication Methods for an Electronic Health Records System*, The 14th International Conference on Health Informatics (HEALTHINF'2021), pp. 20-26.

14. Agnideven Palanisamy Sundar, Feng Li, Xukai Zou, Qin Hu, and Tianchong Gao. *Multi-Armed-Bandit-based Shilling Attack on Collaborative Filtering Recommender Systems*, The International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2020), pp. 347-355.

15. Q. Hu, F. Li, X. Zou, and Y. Xiao, *Correlated Participation Decision Making for Federated Edge Learning*, IEEE GLOBECOM 2020, pp. 1-6.

16. A. P. Sundar, F. Li, X. Zou and T. Gao, *Deep Dynamic Clustering of Spam Reviewers using Behavior-Anomaly-based Graph Embedding*, IEEE GlobalCom 2020, pp. 1-6.

17. Saptarshi Purkayastha, Shreya Goyal, Tyler Phillips, Huanmei Wu, Brandon Haakenson and Xukai Zou, *Continuous Security through Integration Testing in an Electronic Health Records System*, International Conference on Software Security and Assurance (ICSSA 2020). pp. 26-31.

18. Xiaoyuan Yu, Brandon Haakenson, Tyler Phillips, and Xukai Zou, *User-Friendly Design of Cryptographically-EnforcedHierarchical Role-based Access Control Model*,2020 29th International Conference on Computer Communications and Networks (ICCCN), Honolulu, HI, USA, 2020, pp. 1-9.

19. Agnideven Palanisamy Sundar, Feng Li, Xukai Zou, Tianchong Gao, and Evan Russomanno. *Understanding Shilling Attacks and their Detection Traits: A Comprehensive Survey*, IEEE Access, 10.1109/ACCESS.2020.3022962, 2020, Vol. 8, pp. 171703-171715.

20. Tyler Phillips, Xiaoyuan Yu, Brandon Haakenson, Shreya Goyal, Xukai Zou, Saptarshi Purkayastha and Huanmei Wu, *AuthN-AuthZ: Integrated, User-Friendly andPrivacy-Preserving Authentication and Authorization*, The 2nd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS 2020), Dec. 1 –3, 2020 (Virtual), pp. 189–198.

21. H. Ge, S. Y. Chau, V. E. Gonsalves, H. Li, T. Wang, X. Zou, and N. Li, *Koinonia: Verifiable E-Voting with Long-term Privacy*, The 2019 Annual Computer Security Applications Conference (ACSAC 2019), December 9-13, 2019, San Juan, Puerto Rico, pp. 270 - 285.

22. Tyler Phillips, Xiaoyuan Yu, Brandon Haakenson and Xukai Zou, *Design and Implementation of Privacy-Preserving, Flexible and Scalable Role-based Hierarchical Access Control*, The First IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS'19), December 12 - 14, 2019. Los Angeles, California, USA, pp. 46-55.

23. Tyler Phillips, Xukai Zou, Feng Li and Ninghui Li, *Enhancing Biometric-Capsule-based Authentication and Facial Recognition Via Deep Learning*, The ACM Symposium on Access Control Models and Technologies (SACMAT'19), Toronto, Canada, June 4 to 6, 2019, pp. 141-146.

24. Tyler Phillips, Kenneth E. Byrd, and Xukai Zou, *Reexamine the identities of soldiers in an iconic image using deep-learning-based facial recognition techniques*, Military Images, Spring 2019, pp. 60-64.

25. Tianchong Gao, Feng Li, Yu Chen and Xukai Zou, *Local Differential Privately Anonymizing Online Social Networks Under HRG-Based Model*, IEEE Transactions on Computational Social Systems, 5(4), 2018, pp. 1009 - 1020.

26. X. Zou, H. Li, F. Li, W. Peng, and Y. Sui, *Transparent, Auditable, and Stepwise Verifiable Online E-Voting Enabling an Open and Fair Election*, Cryptography, MDPI, Volume 1(2), 2017, pp. 1–29.

27. Tamara Dugan and Xukai Zou, *Privacy-preserving evaluation techniques and their application in genetic tests*, Smart Health, Elsevier, Volume 1(2), June 2017, pp. 2-17.

28. Yefeng Ruan and Xukai Zou, *Receipt-Freeness and Coercion Resistance in Remote E-Voting Systems*, International Journal of Security and Networks, Volume 12(2), 2017, pp. 120-133.

29. T. Gao, F. Li, Y. Chen, and X. Zou, *Preserving Local Differential Privacy in Online Social Networks*, International Conference on Wireless Algorithms, Systems, and Applications (WASA 2017), LNCS Vol. 10251, pp. 393-405.

30. T. Phillips, X. Zou, and F. Li, *A Cancellable and Privacy-Preserving Facial Biometric Authentication Scheme*, IEEE 14th International Conference on Mobile Ad Hoc and Sensor Systems (MASS 2017), pp. 545 - 549.

31. Tamara Dugan and Xukai Zou, *A Survey of Secure Multiparty Computation Protocols for Privacy Preserving Genetic Tests*, 2016 the IEEE 1st International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE 2016), Washington D.C, USA, June 27-29, pp. 173 - 182, 2016.

32. Sahana Shivaprasad, Huian Li and Xukai Zou, *Privacy Preservation in Location Based Services*, Journal of Computers, 11(5), 2016, pp.411-422.

33. Yefeng Ruan, Sivapriya Kalyanasundaram, and Xukai Zou, *Survey of Return-Oriented Programming Defense Mechanisms*, Security and Communication Networks, 2016 (9), pp. 1247–1265.

34. Kevin Butterfield, Huian Li, Xukai Zou, and Feng Li, *Enhancing and Implementing Fully Transparent Internet Voting*, ICCCN'15, August 3 to 6, 2015, pp. 1–6.

35. W. Peng, F. Li and X. Zou, *Temporal Coverage Based Content Distribution in Heterogeneous Smart Device Networks*, ICC 2015, pp. 3477 - 3482.

36. Qiang Wu, Hua Xu, Xukai Zou, Hongzhuan Lei, *A 3D modeling approach to complex faults with multi-source data*, Computers & Geosciences, Volume 77, April 2015, Pages 126–137.

37. K. Butterfield and X. Zou, *Analysis and Implementation of Internet Based Remote Voting*, 2014 IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pp. 714 - 719.

38. H. Li, A. R. Kankanala and X. Zou, *A Taxonomy and Comparison of Remote Voting Schemes*, ICCCN 2014, August 4–7, Shanghai, China, pp. 666–673.

39. M. Rangmala, Z. Liang, W. Peng, X. Zou and F. Li, *A Signature based Mutual Agreement Scheme for Secure Data Provenance*, ICCCN 2014, August 1–7, Shanghai, China, pp. 726–733.

40. W. Peng, F. Li, C. T. Huang, X. Zou *A Moving-target Defense Strategy for Cloud-based Services with Heterogeneous and Dynamic Attack Surfaces*, ICC'2014, pp. 804–809.

41. W. Peng, F. Li, K. Hand and X. Zou, *Moving-target Defense for Cloud Infrastructure: Lessons from Botnets*, High performance semantic cloud auditing and applications, New York: Springer Verlag, Book chapter, pp. 35–64, 2014.

42. X. Zou, H. Li, Y. Sui, W. Peng, and F. Li *Assurable, Transparent, and Mutual Restraining E-voting Involving Multiple Conflicting Parties*, INFOCOM'2014, Toronto, Canada, April 28–May 2, 2014, pp. 136–144.

43. Y. Sui, X. Zou, Y. Du, and F. Li, *Design and Analysis of a highly user-friendly, secure, privacy-preserving, and revocable authentication method*, IEEE Transactions on Computers, 63(4), pp. 902-916, April 2014. doi:10.1109/TC.2013.25.

44. W. Peng, F. Li, X. Zou, and J. Wu, *Behavioral Malware Detection in Delay Tolerant Networks*, IEEE Transactions on Parallel and Distributed Systems, 25 (1), pp. 53–63, 2014.

45. W. Peng, F. Li, X. Zou, and J. Wu, *A Two-stage Deanonymization Attack Against Anonymized Social Networks*, IEEE Transactions on Computers, 63(2), pp. 290–303, 2014.

46. M. Rangwala, P. Zhang, X. Zou and F. Li, *A Taxonomy of Privilege Escalation Attacks in Android Applications*, International Journal of Security and Networks, Vol. 9, No. 1, 2014, pp. 40–55.

47. W. Peng, F. Li, X. Zou, J. Wu, *Offloading Topical Cellular Content through Opportunistic Links*, The Tenth IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2013) , October 14-16, in HangZhou, 2013, ZheJiang Province, P.R.China, pp.402 - 410.

48. H. Li, Y. Sui, W. Peng, X. Zou, and F. Li, *A Viewable E-voting Scheme for Environments with Conflict of Interest*, IEEE Conference on Communications and Network Security (CNS), Oct. 14–16, 2013 Washington, D.C., USA, pp.251 - 259

49. W. Peng, F. Li, K. J. Han, X. Zou, and J.Wu, *T-dominance: Prioritized Defense Deployment for BYOD Security*, IEEE Conference on Communications and Network Security (CNS), Oct. 14–16, 2013 Washington, D.C., USA, pp.37 - 45.

50. Feng Li, Wei Peng, Chin-Tser Huang, and Xukai Zou, *Smartphone Strategic Sampling in Defending Enterprise Network Security*, ICC 2013, Dresden, Germany, pp.2155 - 2159.

51. Y. Sui, X. Zou and Y. Du, *Cancellable Biometrics*, (book chapter), pp. 233–252, in Biometrics: from Fiction to Practice, Pan Stanford Publishing Pte. Ltd.,2013.

52. Y. Sui, X. Zou, Y. Du and F. Li, *Secure and Privacy-preserving Biometrics based Active Authentication*, The 2012 IEEE International Conference on Systems, Man, and Cybernetics (IEEE SMC 2012), pp.1291 - 1296.

53. Y. Sui, X. Zou, F. Li and E. Y. Du, *Active User Authentication for Mobile Devices*,The 7th International Conference on Wireless Algorithms, Systems, and Applications (WASA 2012), pp. 540 - 548.

54. W. Peng, F. Li, X. Zou, and J. Wu, *Seed and Grow: An Attack Against Anonymized Social Networks*, IEEE International Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'12), pp. 587 - 595.

55. W. Peng, F. Li, X. Zou, and J. Wu, *A Privacy-Preserving Social-Aware Incentive System for Word-of-Mouth Advertisement Dissemination on Smart Mobile Devices*, IEEE International Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'12), pp. 596 - 604.

56. F. Li, X. Zou, P. Liu and Y. Chen, *New threats to health data privacy*, BMC Bioinformatics 2011, 12 (Suppl 12):S7 doi:10.1186/1471-2105-12-S12-S7.

57. Pratima Adusumilli, Yan Sui, Xukai Zou,Byrav Ramamurthy, and Feng Li, *A Key Distribution Scheme for Distributed Group with Authentication Capability*, International Journal of Performability Engineering. 8(2), March 2012, pp. 179–192.

58. X. Zou, P. Liu, and J. Chen, *Personal Genome Privacy Protection with Feature-based Hierarchical Dual-stage Encryption*, The 2011 IEEE International Workshop on Genomic Signal Processing and Statistics (GENSIPS'11), San Antonio, Texas, USA, Dec. 4-6. 2011.

59. W. Peng, F. Li, X. Zou and J. Wu, *Behavioral Detection and Containment of Proximity Malware in Delay Tolerant Networks*, The 8th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2011), October 17-22, 2011, Valencia, Spain, Pages 411-420.

60. X. Zou, F. Maino, E. Bertino, Y. Sui, K. Wang, and F. Li, *A New Approach to Weighted Multi-Secret Sharing*, ICCCN 2011, July 31 - August 4, Hawaii, USA.

61. Y. Sui, X. Zou, and Y. Du, *Biometrics-based Authentication: a New Approach*, ICCCN 2011, July 31 - August 4, Hawaii, USA.

62. Xukai Zou, Mingrui Qi, Feng Li, Yan Sui, and Kai Wang, *A New Scheme for Anonymous Secure Group Communication*, 44th Hawaii Int'l Conference on System Sciences (HICSS-44), Kauai, Hawaii, USA, January 4-7, 2011.

63. Y. Wang, B, Ramamurthy, X. Zou, and Y. Xue, *An efficient scheme for removing compromised sensor nodes from wireless sensor networks,* Security and Communication Networks, 3(4): 320-333 (2010).

64. F. Li, Y. Chen, X. Zou and P. Liu, *New Privacy Threats in Healthcare Informatics: When Medical Records Join the Web*, Proceedings of BIOKDD 2010, Washington DC, USA.

65. F. Li, Y. Yang, J. Wu and X. Zou, *Fuzzy Closeness-based Delegation Forwarding in Delay Tolerant Networks*, the 5th IEEE International Conference on Networking, Architecture, and Storage (NAS 2010), pp. 333–340.

66. Y. Sui, K. Yang, Y. Du, S. Orr, and X. Zou, *A novel key management scheme using biometrics*, Proceedings of Mobile Multimedia/Image Processing, Security, and Applications 2010 conference, 5–9 April 2010, Orlando, Florida, USA, Vol. 7708, 77080C (2010).

67. K. Yang, Y. Sui, Z. Zhou, Y. Du, and X. Zou, *A new approach for cancelable iris recognition*, Proceedings of Mobile Multimedia/Image Processing, Security, and Applications 2010 conference, 5–9 April 2010, Orlando, Florida, USA, Vol. 7708, 77080A (2010).

68. Y. Sui, F. Maino, Y. Guo, K. Wang and X. Zou, *An Efficient Time-bound Access Control Scheme for Dynamic Access Hierarchy*, in Proceedings of The Fifth International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2009), 14-16 December 2009, Wu Yi Mountain, China, pp.279 - 286.

69. K. Wang, X. Zou, and Y. Sui, *A Multiple Secret Sharing Scheme based on Matrix Projection*, COMPSAC'09, Seattle, WA, USA, July 20 –24, 2009, pp. 400-405.

70. B. Li and X. Zou, *A Proactive Secret Sharing Scheme in Matrix Projection Method*, International Journal of Security and Networks, 4(4), 2009, pp. 201-209.

71. Y. Dai, X. Li, X. Zou, and L. Xing, *Rebound Wall: A Novel Technology against DoS Attacks,* Special Issue on System Survivability and Defense against External Impacts, International Journal of Performability Engineering, Vol. 5, No. 1, pp. 55-70, January 2009.

72. X. Zou and Li Bai, *A New Class Of Key Management Scheme For Access Control In Dynamic Hierarchies*, International Journal of Computer and Applications, 30(4), 2008, pp. 331-337.

73. S. Magliveras, W. Wei, and X. Zou, *Notes on the CRTDH Group Key Agreement Protocol*, Proceedings of The 28th International Conference on Distributed Computing Systems Workshops (ICDCS'08), Beijing, China, June 17–20, 2008, pp. 406-411. (Note: the authors are listed in the alphabetic order of their last names.)

74. X. Zou, Y. Dai and E. Bertino, *A Practical and Flexible Key Management Mechanism For Trusted Collaborative Computing*, Proceedings of the 27th IEEE INFOCOM, April 13–18, 2008, pp. 1211–1219.

75. Y. Wang, B. Ramamurthy, Y. Xue, and X. Zou, *A Security Framework for Wireless Sensor Networks Utilizing a Unique Session Key*, The 5th International Conference on Broadband Communications, Networks and Systems, 2008 (BROADNETS 2008), pp. 487 - 494.

76. X. Zou and Y. karandikar@, *A Novel Conference Key Management solution for Secure Dynamic Conferencing*, Inter. Journal of Security and Networks, 3(1), 2008, pp. 47–53.

77. R. Balachandran@, X. Zou, B. Ramamurthy, A. Thurkral@, N. V. Vinodchandran, *An Efficient and Attack-resistant Key Agreement Scheme for Secure Group Communications in Mobile Ad-Hoc Networks*, Wireless Communications & Mobile Computing. 8(10), 2008, pp. 1297-1312.

78. X. Zou, Y. karandikar@, E. Bertino, A Dynamic Key Management Solution to Access Hierarchy, International Journal of Network Management, 17(6), 2007, pp. 437–450.

79. X. Zou, Y. Dai, and X. Ran@, *Dual-Level Key Management for Secure Grid Communication in Dynamic and Hierarchical Groups*, Future Generation of Computer Systems, 23(6), 2007, pp. 776–786.

80. Y. Dai, Y. Pan, and X. Zou, *A Hierarchical Modeling and Analysis for Grid Service Reliability*, IEEE Transaction on Computers, 56(5), 2007, pp. 681–691.

81. Y. Wang@, B. Ramamurthy, and X. Zou, *KeyRev: An Efficient Key Revocation Scheme for Wireless Sensor Networks*, Proceedings of IEEE ICC'07, 24-27 June 2007, Glasgow, Scotland, pp.1260 - 1265.

82. Y. Karandikar@, X. Zou and Y. Dai, *An Effective Key Management Approach to Differential Access Control in Dynamic Environments*, Journal of Computer Science, 2(6):542–549, 2006.

83. X. Zou, A. Thukral@, and B. Ramamurthy, *An Authenticated Key Agreement Protocol for Mobile Ad Hoc Networks*, LNCS, Springer, Vol. 4325, pp. 509–520, (The 2nd International Conference on Mobile Ad-hoc and Sensor Networks (MSN06), Hong Kong, China, 12/13–12/15, 2006.

84. X. Zou and Y. Dai, *A Robust and Stateless Self-Healing Group Key Management Scheme*, Proceedings of The 2006 IEEE International Conference on Communication Technology, Guilin, China, Nov. 28–30, 2006, pp. 455–459.

85. Y. Wang@, B. Ramamurthy, and X. Zou, *The Performance of Elliptic Curve Based Group Diffie-Hellman Protocols for Secure Group Communication over Ad Hoc Networks*, the Proceedings of IEEE ICC 2006, 11-15 June 2006, Istanbul, TURKEY, Vol.5, pp.2243 - 2248.

86. S. Deshpande@, A. Todimala@, R. K Balachandran@, B. Ramamurthy, X. Zou, and N. V. Vinodchandran, *A New Cryptographic Scheme for Securing Dynamic Conferences in Data Networks*, the Proceedings of IEEE ICC 2006, 11-15 June 2006, Istanbul, TURKEY, vol. 5, pp.2310 - 2315.

87. Q. Wu, Hua Xu, and X. Zou, *An Effective Method for 3D Geological Modeling with Multi-source Data Integration*, Computers & Geosciences, 31(1) , Feb. 2005, pp. 35-43.

88. A. Thukral@ and X. Zou, *Secure Group Instant Messaging based on Cryptographic Primitives*, Lecture Notes in Computer Science (LNCS), Springer-Verlag, Vol. 3619, pp. 1002-1011, August, 2005. (The 2005 International Conference on Computer Networks and Mobile Computing) (ICCNMC'05).

89. Y. Dai, X. Zou and Y. Guo@, *Grid-Based Information System with Fault Tolerance, Self-Healing and High-Performance*, the Proceedings of 10th Annual International Conference on Industrial Engineering Theory, Applications and Practice, Florida, December 4-7, 2005, pp. 455-460.

90. G. Hao@, N. V. Vinodchandran, B. Ramamurthy and X. Zou, *A Balanced Key Tree Approach for Dynamic Secure Group Communication*, Proceedings of ICCCN 2005 Fourteenth International Conference on Computer Communications and Networks (ICCCN), October 17-19, 2005, CA, USA, pp. 345–350.

91. P. Adusumilli@, X. Zou and B. Ramamurthy, *DGKD: Distributed Group Key Distribution with Authentication Capability*, Proceedings of the 2005 IEEE Workshop on Information Assurance (IAW), United States Military Academy, West Point, NY, 15-17 June 2005, pp. 286–293.

92. Y. Karandikar@, X. Zou and Y. Dai, *Secure Group Communication Based Scheme for Differential Access Control in Dynamic Environments*, Proceedings of The 1st IEEE Workshop on Reliability and Autonomic Management In Parallel and Distributed Systems (RAMPDS-2005), 2005, pp. 448–453.

93. P. Adusumilli@ and X. Zou, *KTDCKM-SDC: A Distributed Conference Key Management Scheme for Secure Dynamic Conferencing*, Proceedings of The Tenth IEEE Symposium on Computers and Communications (ISCC), Cartagena, Spain, June 27-30, 2005, pp. 476–481.

94. R. K. Balachandran@, B. Ramamurthy, X. Zou, and N. V. Vinodchandran, *CRTDH: An Efficient Key Agreement Scheme for Secure Group Communications in Wireless Ad-Hoc Networks*, Proceedings of IEEE International Conference on Communication (ICC) 2005, pp. 1123–1127.

95. X. Zou and B. Ramamurthy, *A Simple Group Diffie-Hellman Key Agreement Protocol without Member Serialization*, Lecture Notes in Computer Science (LNCS),

Springer-Verlag, Vol. 3314, pp. 725-731, December 2004. (The 2004 International Symposium on Computational and Information Sciences).

96. X. Zou, S. Magliveras and B. Ramamurthy, *Key Tree based Scalable Secure Dynamic Conferencing Schemes*, Proceedings of International Conference on Parallel and Distributed Computing and Systems (PDCS'04), MIT Cambridge, MA, USA, Nov. 2004, pp. 61–65.

97. X. Zou and B. Ramamurthy, *A Block-Free Tree Based Group Diffie-Hellman Key Agreement Protocol for Secure Group Communication*, Proceedings of International Conference on Parallel and Distributed Computing and Networks, Innsbruck, Austria, February 17-19, 2004, pp. 288–293.

98. X. Zou, B. Ramamurthy, V. Variyam and R. K. Balachandran@, *Algorithms for Unified Hierarchy Based Access Control*, Proceedings of International Conference on Communications, Internet, & Information Technology (CIIT 2003), Scottsdale, AZ, USA, November 17-19, 2003, pp. 31–36.

99. X. Zou, B. Ramamurthy and S. Magliveras, *Efficient Key Management for Secure Group Communication with Bursty Behavior*, Proceedings of International Conference on Communication, Internet, and Information Technology, Virgin Islands, USA, November 2002, pp. 148–153.

100. X. Zou, B. Ramamurthy and S. Magliveras, *Chinese Remainder Theorem based Hierarchical Access Control for Secure Group Communications*, Lecture Notes in Computer Science (LNCS), Springer-Verlag, vol. 2229 (2001), pp. 381–385.

101. X. Zou, B. Ramamurthy and S. Magliveras, *Routing Techniques for Wireless Ad hoc Networks– Classification and Comparison*, Proceedings of the Sixth World Multiconference on Systemics, Cybernetics, and Informatics, Florida, USA, July, 2002, pp. 352-357.

102. J.-C. Birget, X. Zou, G. Noubir and B. Ramamurthy, *Hierarchy-based Access Control in Distributed Environments*, Proceedings of IEEE International Conference on Communications, June 2001, Helsinki, Finland, pp. 229–233.

103. X. Zou, S. Magliveras and B. Ramamurthy, *A Dynamic Conference Scheme Extension with Efficient Burst Operations*, Congressus Numerantium, Vol. 158, 2002, pp. 83–92.

104. X. Zou, *An Efficient Approach to Computing the Edit Distance and Edit Path for char/(Chinese Character) String.* Computer Research and Development, 33 (8), 1996, pp 574–581.

105. X. Zou, *An Efficient Edit Distance and Edit Path Computation Approach.* Mini-Micro Systems, 17(7), 1996, pp 72–76.

106. X. Zou and S. Wang, *An Efficient Parallel Approximate Approach to Char/(Chinese Characters) String Pattern Matching.* Journal of Advanced Software Research, 2(2), 1995, pp 198–203.

107. X. Zou and S. Wang, *A Fast Approach to Char/(Chinese Characters) String Pattern Matching Allowing Errors*. Journal of Advanced Software Research, 2(2), 1995, pp 147–152.

108. S. Wang and X. Zou, *An Approach for Parallel String Pattern Matching Allowing Errors*. Computer Research and Development, 32(2), 1995, pp 34–38.

109. X. Zou and S. Wang, *An Efficient Parallel Approximate Approach to Char/(Chinese Characters) String Pattern Matching*. Journal of Software, 6(8), 1995, pp 463–468.

110. S. Wang and X. Zou, *An Optimal Parallel Chinese Character/Char String Searching Approach*. Journal of Chinese Information Processing. 6(1), 1995, pp. 23-28.

111. X. Zou and S. Wang, *An Efficient Approach to Automatic Checking and Correction of Spelling Errors in Compilation*. Journal of Zhengzhou University, 27(1), 1995.

112. X. Zou and S. Wang, *A Fast Approach to Char/(Chinese Characters) String Pattern Matching Allowing Errors*. Journal of Software, 5(10), 1994, pp 55–59.

113. X. Zou and S. Wang, *An Optimal Parallel String Searching Approach*. Journal of Zhengzhou University, 26(1), 1994, pp 41–45.

114. X. Zou and S. Wang, *A Fast Approach to Char/(Chinese Character) String Pattern Matching*. Mini-Micro Systems. 14(11), 1993, pp 49–53.

115. X. Zou and Y. Guo, *A Reliable Microcomputer Communication Approach*. Journal of Zhengzhou University, 25(3), 1993, pp24–28.

116. X. Zou, *Notes on McCabe Approach to Measuring Program Complexity*. Henan Electronics Technology, 4(1), 1993, pp. 31–37.

117. S. Wang and X. Zou, *An Efficient Parallel Approximate Approach to Char/Chinese Character String Searching*, Journal of Advanced Software Research, 2(2), 1995, pp. 198–203.

118. X. Zou and S. Wang, *A Fast Approach to Char/Chinese Characters Text Searching Allowing Errors*, Journal of Advanced Software Research, 2(2), 1995, pp. 147–152.

5.3 Other manuscripts

119. K. Wang@, Y. Sui@, X. Zou, A. Durresi, and S. Fang, *Pervasive and Trustworthy Healthcare*. The First IEEE International Workshop on Bio Computing (BioCom'08), Okinawa, Japan, March 25 - 28, 2008, pp. 750–755.

120. (Extended Abstract) X. Zou, Y.S. Dai, B. Doebbeling, M. Qi@, *Dependability and Security in Medical Information System*, the 12th International Conference on Human-Computer Interaction, 2007, Lecture Notes of Computer Science (LNCS), vol. 4553, pp. 316-326.

121. Y.-S. Dai, M. Hinchey, M. Madhusoodan@, J. L. Rash, and X. Zou, *A Prototype Model for Sefl-Healing and Self-Reproduction in Swarm Robotic System*, Proceedings of The 2nd IEEE International Symposium on Dependable, Autonomic, and Secure Computing, Indianapolis, IN, USA, Sept. 29 - Oct. 1, 2006, pp. 3–10.

122. Y.-S. Dai, M. Hinchey, M. Qi@, and X. Zou, *Autonomic Security and Self-Protection based on Feature-Recognition with Virtual Neurons*, Proceedings of The 2nd IEEE International Symposium on Dependable, Autonomic, and Secure Computing, Indianapolis, IN, USA, Sept. 29 - Oct. 1, 2006, pp. 227–234.

123. O. Tilak@, R. Raje, and X. Zou, *Composing Access Control in Distributed Systems*, The 2nd IEEE International Symposium on Dependable, Autonomic, and Secure Computing, Indianapolis, IN, USA, Sept. 29 - Oct. 1, 2006, pp. 301–307.

124. (Invited book chapter) X. Zou, A. Thukral@, and Y. Karandikar@ *Security Issues and Techniques in Trusted Collaborative Computing (TCC)*, Parallel and Distributed Computing: Evaluation, Improvement and Applications, Editors, Y. Dai, Y. Pan, and R. Raje, Nova Science Publishers, 2006, ISBN: 1-60021-202-6, pp. 31–54.

125. (Peer-reviewed book chapter) X. Zou, *Public Key Standards: SSH (Secure Shell)*, The Handbook of Information Security, Hossein Bidgoli, Editor-in-Chief, John Wiley & Sons Inc., 2005, ISBN: 978-0-471-64833-8, Vol. 1, pp. 979–994.

126. (Peer-reviewed book chapter) X. Zou and A. Thukral@, *Key Management*, The Handbook of Information Security, Hossein Bidgoli, Editor-in-Chief, John Wiley & Sons Inc., 2005, ISBN: 978-0-471-64833-8, Vol. 2, pp. 636–646.

127. (Poster) X. Zou, B. Ramamurthy, and S. S. Magliveras, *A GCD Attack Resistant CRTHACS for Secure Group Communications*, Proceedings of International Conference on Information Technology, ITCC 2004, April 5 -7, 2004, Las Vegas, NV, USA, pp. 153–154.

128. (Monograph) X. Zou, C. Yang, H. Li and F. Liang, *Intranet Technologies and Applications*, ISBN 7-5606-0613-X, Xian Electronic Sci. and Tech. Univ. Publishing Press, Aug. 1998.

6 Courses taught and Winner of IUPUI Trustees' Teaching Award three times

Cryptography, Network Security, Advanced Information Assurance, Communication and Data Network, Data Structures, Design and Analysis of Algorithms, Programming Languages, and Compiler.

7 Recognition and awards

- University Trustees Teaching Award, IUPUI, 2021.
- University Trustees Teaching Award, IUPUI, 2013.
- University Trustees Teaching Award, IUPUI, 2008.
- University Outstanding teaching achievement award and Outstanding young researcher, Zhengzhou University, 1996.

- University Outstanding teaching achievement award, Zhengzhou University, 1994.
- Fellow of Indiana University' Center for Applied Cybersecurity Research (CACR), 2010.
- Fellow of Indiana University' Center for Applied Cybersecurity Research (CACR), 2009.
- Featured on CBS4 news for Fighting Fraud: CBS4 investigates how often hackers, scammers are hitting Hoosiers.
- Featured on Fox News 59 for a security breach at Anthem, the insurance company based in Indianapolis. The interview video can be found at http://www.fox59.com/news/wxin-anthem-letters-062510,0,1566956.story.
- Featured by news "IUPUI Computer Scientists Develop Revolutionary Medical Information System" at http://www.iupui.edu/news/releases/060222_med_info_system.htm, 2006.
- National scientific and technological achievement, awarded by Chinese Science and Technology Committee, 1996.
- Excellent author of scientific and technical articles, by Science and Technology Committee of Henan Province in 1996 and 1998.
- Outstanding graduate, by Zhengzhou University, 1983 (**only one in the entire graduating class of about 30 students each year**).

8 Presentations

(a) Invited presentations

1. *A Verifiable, Transparent and Assurable Remote Electronic Voting System and its Application to Cybersecurity Education*, ALABAMA IEEE COMPUTER SOCIETY amd THE UNIVERSITY OF ALABAMA, DEPARTMENT OF COMPUTER SCIENCE, 3/1/2022.
2. *Revocable, Privacy-preserving, and User-centric (Active) Authentication based on Biometric-Capsule*, NSF S2ERC center 2015 showcase, 12/11/2015.
3. *SECURE, PRIVACY-PRESERVING AND CANCELABLE BIOMETRIC AUTHENTICATION: A BIO-CAPSULE APPROACH*, IEEE EnCon Conference, November 7, 2014, Indianapolis, Indiana (Central Indiana Section (CIS) of IEEE).
4. *Personal Genomic Data Security and Privacy: controlled sharing with fine-tuned access confinement*, 2012 Translational Informatics Conference, IUPUI, April 26-27, 2012.
5. *High assured and trusted collaborative computing platform*, Raytheon Day, CERIAS, Purdue University, Nov. 2, 2011.
6. *Weighted Multiple Secret Sharing*, Purdue University, CERIAS, Sept. 28, 2011.

7. *Authentication and Key Management for secure (anonymous) group communication*, Temple University, Feb. 18, 2011.

8. *Secure and seamless medical information system*, the 47th S2ERC Showcase (Security and Software Engineering Research Center), Ball State University, Nov. 12, 2009.

9. *Multiple Secret Sharing with Weighted Shares*, Codes, Designs, and Finite Group Conference, Florida, May 20, 2009.

10. *A Uniform Approach to Secure Group Communication and Hierarchical Access Control*, College of Information Engineering, Zhengzhou University, China, June 20, 2008.

11. *Access Control Polynomial based Security Support for Trusted Collaborative Computing (TCC)*, Department of Computer Science, Georgia State University, May 13, 2008.

12. *Secure and Seamless Medical Information System*, An Open House for Center for Mathematical Biosciences & Center for Bio-Computing, Friday, October 26, 2007.

13. *Cryptography based Hierarchical Access Control*, Department of Computer Science, Indiana University-Purdue University Fort Wayne, March 13, 2007.

14. *Trusted Collaborative Computing*, Department of Computer Science and Engineering, Florida Atlantic University, March 30, 2006.

15. *Cryptography and Network Security*, College of Information Engineering, Zhengzhou University, China, December 27, 2004.

(b) Conference presentations

16. *User-Friendly Design of Cryptographically-EnforcedHierarchical Role-based Access Control Model*, IEEE ICCCN 2020 (Virtual).

17. *Enhancing Biometric-Capsule-based Authentication and Facial Recognition Via Deep Learning*, The ACM Symposium on Access Control Models and Technologies (SACMAT'19), Toronto, Canada,

18. *Assurable, Transparent, and Mutual Restraining E-voting Involving Multiple Conflicting Parties*, INFOCOM'2014, Toronto, Canada, April 28 –May 2, 2014.

19. *A New Approach to Weighted Multi-Secret Sharing*, ICCCN 2011, July 31 - August 4, Hawaii, USA.

20. *Biometrics-based Authentication: a New Approach*, ICCCN 2011, July 31 - August 4, Hawaii, USA.

21. *A New Scheme for Anonymous Secure Group Communication*, 44th Hawaii Int'l Conference on System Sciences (HICSS-44), Kauai, Hawaii, USA, January 4-7, 2011.

22. *A Multiple Secret Sharing Scheme based on Matrix Projection*, COMPSAC'09, Seattle, Washington, USA, April 23, 2009.

23. *Notes on the CRTDH Group Key Agreement Protocol*, The First International Workshop on Wireless Security and Privacy (WiSP'08), held in conjunction with The 28th International Conference on Distributed Computing Systems (ICDCS'08), Beijing, China, June 17–20, 2008.

24. *A Practical and Flexible Key Management Mechanism For Trusted Collaborative Computing*, IEEE INFOCOM 08, Phoenix, AZ, USA, April 13–18, 2008.

25. *A Robust and Stateless Self-Healing Group Key Management Scheme*, The 2006 IEEE International Conference on Communication Technology, Guilin, China, Nov. 28–30, 2006,

26. *DGKD: Distributed Group Key Distribution with Authentication Capability*, The 2005 IEEE Workshop on Information Assurance (IAW), United States Military Academy, West Point, NY, USA, 16 June 2005.

27. *A Simple Group Diffie-Hellman Key Agreement Protocol without Member Serialization*, The International Conference on Computational and Information Sciences (CIS'04), December, 2004.

9 Professional services

- NSF Panelist, 2008, 2009, 2016. NIH Grand Challenge Grant reviewer, 2009.
- **Sitting on Boards and Committees**
  - Associate Editor, ACM Transactions on Privacy and Security (TOPS), June 2023, —>
  - Guest Editor, Special Issue "Cybersecurity in Deep Learning with Big Data" for International Journal Frontiers In Big Data, Jan. 2023 to Jan. 2024.
  - Invited Editor, SAGE Open, (2018)
  - Invited Reviewer, Computing Review, (2014 -)
  - Associate Editor, International Journal of Communications, (2011-)
  - Associate Editor, International Journal of Security and Networks (2009-).
  - Associate Editor, International Journal of Computers and Applications (2003-13).
  - Program Co-Chair, Vice Chair, Finance Chair, Local Arrangement Chair, Conference Session Chair, and Technical Committee Member on many international conferences, most recent including ACM SACMAT 2017.
- **Reviewer**
  - Reviewer for over 40 international journals including IEEE Transactions on Computers, IEEE Transaction on Dependable and Secure Computing (IEEE TDSC), ACM Transactions on Privacy and Security (ACM TOPS) (formerly known as ACM Transactions on Information and System Security).
  - Reviewer for over 60 international conferences.
- Professional Membership: ACM, and IEEE computer society.