Xukai Zou’s Curriculum Vitae

1 Education

- PhD in Computer Science, University of Nebraska-Lincoln, 12/2000.
- MS in Computer Science, Huazhong University of Science and Technology, China, 06/1986.
- BS in Computer Science, Zhengzhou University, China, 07/1983.

2 Academic appointments

- Aug. 2009 - Present: Associate Professor
  Department of Computer and Information Science, Indiana University-Purdue University Indianapolis, IN, USA.

- Aug. 2003 - Jul. 2009: Assistant Professor
  Department of Computer and Information Science, Indiana University-Purdue University Indianapolis, IN, USA.

  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

  ACE Information Resource Inc., Fort Lee, NJ, USA.

  Dept. of Computer Science and Engineering, University of Nebraska-Lincoln, NE, USA.

3 Research interests

Applied cryptography, information security, networking/network security, wireless & mobile security, (biometric) authentication, health informatics & data privacy, and design & analysis of algorithms.

4 Publications

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


4.2 Peer-reviewed articles

3. # Sahana Shivaprasad, Huian Li and Xukai Zou, Privacy Preservation in Location Based Services, Journal of Computers.(In Press)

4. # Kevin Butterfield, Huian Li, Xukai Zou, and Feng Li, Enhancing and Implementing Fully Transparent Internet Voting, MobiPST Workshop, ICCCN 2015 (accepted).

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


30. # 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.


32. # 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.


43. # 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.)


### 4.3 Other manuscripts


5 Recognitions and awards

- # Trustees Teaching Award, IUPUI, 2013.
- # 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.
- # Fellow of Indiana University’ Center for Applied Cybersecurity Research (CACR), 2010.
- # Fellow of Indiana University’ Center for Applied Cybersecurity Research (CACR), 2009.
- # Trustees Teaching Award, IUPUI, 2008.
• 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 teaching achievement award, 1994 and Outstanding young researcher, 1996, by Zhengzhou University.

• Outstanding teaching achievement award, by Zhengzhou University in 1994.

• Outstanding graduate, by Zhengzhou University, 1983.

6 Grants

(a) External


2. # Northrop Grumman, MovingCloud: Create Moving-target Defense in Cloud by Learning from Botnets, 10/1/2012–9/31/2013, with F. Li.


4. # NSF, Secure Group Communications over Wired/Wireless Networks, (CCR-0311577), 08/01/03 - 07/31/07, with B. Ramamurthy and V. Variyam.

5. # Department of Veterans Affairs, Secure and Reliable Medical Information Systems, 01/01/06 - 12/31/07, with Y. Dai.


(b) Internal

7. # Purdue University Summer Research Grant, Research and Evaluation of Privacy-Preserving and Replaceable Biometrics-based Authentication, 2011.

8. # 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, with J. Chen.

9. # Indiana University’s Center for Applied Cybersecurity Research (CACR) Grant, A novel approach to resilient, secure, and cancellable biometrics, 07/01/09–07/31/10, with E. Y. Du and S. Orr.

11. # IUPUI RSFG grant, *Secure and Dependable Medical Information System*, 12/15/05 - 12/15/06, with Y. Dai.


13. # Trusted Collaborative Computing and Robust Group Key Management, Granted by IU seed fund, 08/01/03 - 06/31/06.

7 Presentations

(a) Invited presentations


3. # High assured and trusted collaborative computing platform, Raytheon Day, CERIAS, Purdue University, Nov. 2, 2011.

4. # Weighted Multiple Secret Sharing, Purdue University, CERIAS, Sept. 28, 2011.

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

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


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


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

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


(b) Conference presentations
15. # A New Approach to Weighted Multi-Secret Sharing, ICCCN 2011, July 31 - August 4, Hawaii, USA.
17. # 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.
18. # A Multiple Secret Sharing Scheme based on Matrix Projection, COMPSAC’09, Seattle, Washington, USA, April 23, 2009.
19. # 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.
20. # A Practical and Flexible Key Management Mechanism For Trusted Collaborative Computing, IEEE INFOCOM 08, Phoenix, AZ, USA, April 13–18, 2008.
21. # A Robust and Stateless Self-Healing Group Key Management Scheme, The 2006 IEEE International Conference on Communication Technology, Guilin, China, Nov. 28–30, 2006,

8 Professional services


• Sitting on Boards and Committees
  – # Invited reviewer, Computing Review.
  – # 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-).
  – # Program Co-Chair, Vice Chair, Finance Chair, and committee member on many international conferences.

• Reviewer
- # Reviewer for over 100 international conferences.

- Professional Membership: ACM, IEEE computer society, and International Association of Science and Technology Development (IASTED).