

1 Curriculum Vitae

Name

Xukai Zou

Education

- PhD in Computer Science, University of Nebraska-Lincoln, December 2000.
- MS in Computer Science, Huazhong University of Science and Technology, China, June 1986.
- BS in Computer Science, Zhengzhou University, China, July 1983.

Academic Appointments

- *Aug. 2003 - current*: Assistant Professor
Department of Computer and Information Science, IUPUI, Indianapolis, IN, USA.
- *Jul. 2002 - Jul. 2003*: Post Doctoral Associate and Lecturer
Dept. of Computer Science and Engineering, University of Nebraska-Lincoln, Lincoln, NE, USA.
- *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, Lincoln, NE, 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.

Professional Services

- **Sitting on Boards and Committees**
 - Technical Program Committee Member, The 2005 International Conference on High Performance Computing and Communications, Sorrento (Naples) , ITALY – September 21 / 23, 2005.
 - Technical Program Committee Member, 2005 International Workshop on Wireless and Sensor Networks Security, held in conjunction with The 2nd IEEE International Conference on Mobile Ad-hoc and Sensor Systems November 7-10, 2005, Wyndham City Center Hotel Washington, DC.
 - Program and Finance Chair, The 2nd International Symposium on Dependable, Autonomic, and Secure Computing (DASC'06).
 - Technical Program Committee member, The First International Workshop on Security in Ubiquitous Computing Systems (SecUbiq-05).
 - Technical Program Committee Co-Chair, The First International Workshop on Trusted and Autonomic Ubiquitous and Embedded Systems (TAUES'05), Nagasaki, Japan, 6-9 December 2005.
 - Technical Program Committee Member, The 1st IEEE Workshop on Reliability and Autonomic Management In Parallel and Distributed Systems (RAMPDS'05), 2005.

- Editorial-Board-Member/Associate Editor (AE) of IASTED/ACTA International Journal of Computers and Applications (2003-).
- IASTED technical committee member on Parallel & Distributed Computing & Systems (2002-2005).
- International Program Committee member for IASTED PDCS 2003, 2004, 2005 conferences.

- **Reviewer:**

- The 2005 International Conference on High Performance Computing and Communications, Sorrento (Naples) , ITALY – September 21 / 23, 2005.
- IEEE 2005 ELECTRO/INFORMATION TECHNOLOGY CONFERENCE (EIT 2005), May 22-25, 2005, University of Nebraska - Lincoln, Lincoln, Nebraska, U.S.A.
- The 2005 International Conference on Computer Networks and Mobile Computing (ICCNMC'05).
- The 1st IEEE Workshop on Reliability and Autonomic Management In Parallel and Distributed Systems (RAMPDS'05), 2005.
- International Conference on Computer Networks and Mobile Computing, 2005.
- The Tenth ACM symposium on access control models and technologies (SACMAT), 2005.
- World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI), 2005.
- International conference on Network and Communication System (NCS), 2005.
- Journal of Systems and Software, 2004.
- Handbook of Information Security, 2004, 2005.
- International Conference on Communication Systems (ACIT-CS) 2005.
- IASTED Systemics, Cybernetics, Informatics (SCI), 2004 -2005.
- Networks, Parallel and Distributed Processing, and Applications (NPDPA), 2004-2005.
- Communication Systems and Networks (CSN) (2004-2005).
- Communications and Computer Networks (CCN) (2004).
- Parallel & Distributed Computing & Systems (PDCS) (2004-2005).
- International Conference on Information and Communication Security (ICICS) (2004).
- Third International Trusted Internet Workshop (TIW) (2004).

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

University Service

- Ph.D. qualifying examination committee, CIS Department, IUPUI, 2003-2005.
- Graduate committee member, CIS Department, IUPUI, 2003-2005.
- University library committee member, IUPUI, 2003-2005.
- Faculty search committee member, 2005.

Grants

(a) External

- *Secure group communications over wired/wireless networks*, NSF, \$350,000.00, 08/01/03 - 07/31/06, (PI: Xukai Zou at IUPUI) (In collaboration with Dr. B. Ramamurthy (PI) and V. Variyam (CO-PI) from University of Nebraska-Lincoln.

(b) Other External Grants

- *The 2nd IEEE Symposium on Dependable Autonomic and Secure Computing (DASC06)*, Indiana University Purdue University at Indianapolis, Granted by IEEE and NASA, \$15,430.00, X. Zou (CO-PI) with Dr. Y. Dai (PI).

(c) Internal

- *Trusted Collaborative Computing and Robust Group Key Management*, Granted by IU seed fund, \$75,000.00, 08/01/03 - 06/31/06, (PI: X. Zou).

Publications

(a) Books

- X. Zou, B. Ramamurthy and Spyros Ramamurthy, *Secure Group Communication over Data Networks*, Springer, ISBN: 0-387-22970-1 (The ebook ISBN: 0-387-22971-X), October 2004, pages 172.
- X. Zou, C. Yang, H. Li and F. Liang, *Intranet technologies and applications*, ISBN 7-5606-0613-X, Xian Electronic Science and Technology University Publishing Press, August 1998.

(b) Book Chapters

- X. Zou, *Public Key Standards: SSH (Secure Shell)*, The Handbook of Information Security, Hossein Bidgoli, Editor-in-Chief, to be published by John Wiley & Sons, Inc, February 2005.
- X. Zou and A. Thukral, *Key management*, The Handbook of Information Security, Hossein Bidgoli, Editor-in-Chief, to be published by John Wiley & Sons, Inc, February 2005.
- X. Zou, A. Thukral, and Y. Karandikar *Secure Group Communication*, Parallel and Distributed Computing: Evaluation, Improvement and Applications, Editors, Y. Dai, Y. Pan, and R. Raje, to be published by Nova Science Publishers, Sept., 2005.

(c) Journal Articles

1. Y. Karandikar@, X. Zou and Y. Dai, *An Effective Key Management Approach to Differential Access Control in Dynamic Environments*, Journal of Computer Science (in press), 2005.
2. Amandeep Thukral@ and Xukai Zou, *Secure Group Instant Messaging based on Cryptographic Primitives*, To appear in Lecture Notes in Computer Science (LNCS), Springer-Verlag, (2005).
3. 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 (2004), pp. 725-731.

4. Q. Wu, Hua Xu, and X. Zou, *An effective method for 3D geological modeling with multi-source data integration*, Computers & Geosciences, 31(1) , February 2005, pp. 35-43.
5. 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.
6. X. Zou, S. Magliveras and B. Ramamurthy, *A dynamic conference scheme extension with efficient burst operation*, Congressus Numerantium, Vol. 158, 2002, pp. 83–92.
7. X. Zou, An efficient approach to compute the edit distance and edit path for char/(Chinese character) string. Computer Research and Development, 33 (8), 1996, pp 574–581.
8. X. Zou, An efficient edit distance and edit path computation approach. Mini-Micro Systems, 17(7), 1996, pp 72–76.
9. 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.
10. 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.
11. S. Wang and X. Zou, An approach for parallel string pattern matching allowing errors. Computer Research and Development, 32(2), 1995, pp 34–38.
12. 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.
13. S. Wang and X. Zou, An optimal parallel Chinese character/char string searching approach. Journal of Chinese Information. 1, 1995.
14. 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.
15. 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.
16. X. Zou and S. Wang, An optimal parallel string searching approach. Journal of Zhengzhou University, 26(1), 1994, pp 41–45.
17. S. Wang and X. Zou, An fast pattern matching approach with scaling. Journal of Zhengzhou University, 26(3), 1994,
18. X. Zou and S. Wang, String searching: theory and practice. in Proceedings of the Fourth young computer scientist annual conference, China, 12, 1994.
19. X. Zou and S. Wang, A fast approach to char/(Chinese character) string pattern matching. Mini-Micro Systems. 14(11), 1993, pp 49–53.
20. X. Zou and Y. Guo, A reliable microcomputer communication approach. Journal of Zhengzhou University, 25(3), 1993, pp24–28.
21. X. Zou, Notes on McCabe approach measuring program complexity. Henan Electronics Technology, 4(1), 1993.

(d) Journal Articles Under Review

1. X. Zou, *An Elegant Bottleneck-free General Hierarchical Access Control Scheme for Highly Dynamic Environments*, Submitted to ACM Transactions on Information and System Security.
2. X. Zou and Y. Karandikar, *A Novel Key Management Scheme for Highly Dynamic Collaborative Environments*, Submitted to International Journal of Information Security (Springer).
3. Y. Karandikar and X. Zou and E. Bertino, *An Efficient and Practical Solution to the Hierarchical Access Control Problem*, Submitted to IEEE Transaction on Dependable and Secure Computing.
4. Y. Karandikar and X. Zou, *A Novel Conference Key Management Solution for Secure Dynamic Conferencing*, Submitted to International Journal of Security and Networks.
5. Y. Dai, Y. Pan, and X. Zou, *Grid Service Reliability Models and Evaluation*, Submitted to IEEE Transactions on Computers.

(f) Refereed Conference Proceeding Papers

1. G. Hao@, N. V. Vinodchandran, B. Ramamurthy and X. Zou, *A Balanced Key Tree Approach for Dynamic Secure Group Communication*, Accepted by ICCCN 2005 FOURTEENTH INTERNATIONAL CONFERENCE ON COMPUTER COMMUNICATIONS AND NETWORKS, October 17-19, 2005, CA, USA.
2. 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.
3. Y. Karandikar@, X. Zou and Y. Dai, *Secure Group Communication Based Scheme for Differential Access Control in Dynamic Environments*, Accepted by The 1st IEEE Workshop on Reliability and Autonomic Management In Parallel and Distributed Systems (RAMPDS-2005), 2005.
4. P. Adusumilli@ and X. Zou, *KTDCM-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.
5. 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*, Accepted by IEEE International Conference on Communication (ICC) 2005.
6. 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 2004), MIT Cambridge, MA, USA, November 2004, pp. 61–65.
7. 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 (Poster), April 5 -7, 2004, Las Vegas, NV, USA, pp. 153–154.
8. 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.
9. 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.

10. 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.
11. 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, Orlando, Florida, USA, July, 2002, pp. 352–357.
12. 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.

(e) Conference articles under review

1. P. Adusumilli and X. Zou, *Symmetric Polynomial based Hierarchical Conference Key Management*, Submitted to International Conference on Information and Communication Security (ICICS'05).

Presentations

(a) Invited Presentations

- Cryptography and network security, College of Information Engineering, Zhengzhou University, China, December 27, 2004.

(b) Conference Presentations

1. *DGKD: Distributed Group Key Distribution with Authentication Capability*, The 2005 IEEE Workshop on Information Assurance (IAW), United States Military Academy, West Point, NY, 16 June 2005.
2. *A simple group Diffie-Hellman key agreement protocol without member serialization*, The International Conference on Computational and Information Sciences (CIS'04), December, 2004.
3. *Secure Group Communication Over the Internet*, Third Annual Regional Workshop in the Mathematical Sciences, University of Nebraska-Lincoln, October, 2000.
4. *An Secure Dynamic Conferencing Scheme with Efficient Bursty Operation*, Thirty Third Southeastern International Conference on Combinatorics, Graph Theory and Computing, March, Boca Raton, Florida, USA, 2002.
5. *Efficient key management for secure group communication with bursty behavior*, International Conference on Communication, Internet, and Information Technology, Virgin Islands, USA, November 2002.

Honors and Awards

- National scientific and technological achievement, awarded by Chinese Science and Technology Committee in 1996.
- Excellent author of scientific and technical articles, by Science and Technology Committee of Henan Province in 1996 and 1998.
- Outstanding young researcher, by Zhengzhou University in 1996.

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