Di Ma

CIS 142
University of Michigan-Dearborn
4901 Evergreen Road
Dearborn, MI 48128

Phone: (313) 583-6737
Fax: (313) 593-4256
Email: dmadma@umich.edu
Web: www.madi.net

RESEARCH INTERESTS

Computer/Network Security & Privacy, Data and Storage Security, and Applied Cryptography

EDUCATION

Ph.D in Computer Science 2009
University of California, Irvine
Dissertation topic: Intrusion Resilience for Unattended Devices
Advisor: Prof. Gene Tsudik

M.E. in Computer Engineering 2000
Nanyang Technological University, Singapore

B.E. in Computer Science 1995
Xi'an Jiaotong University, China

HONORS AND AWARDS

2012	Travel Grant, Aspiring PI Workshop, sponsored by NSF
2011	Air Force Summer Faculty Fellowship (SFFP), sponsored by Air Force Office of Scientific Research (AFOSR)
2010	Travel Grant, 30th International Conference on Distributed Computing Systems (ICDCS 2010)
2009	NSF-TRUST Fellowship, sponsored by NSF
2009	Travel Grant, CRA-W Career Mentoring Workshop, sponsored by NSF
2009	Graduate Dean's Dissertation Fellowship, Graduate Division, UC Irvine
2008	Travel Grant, 10th Symposium on Stabilization, Safety and Security of Distributed Systems (SSS'08)
2008	Invited Participant, Cyber Physical Systems Security workshop, supported by ARO
2008	Travel Grant, Faculty Horizons at UMBC, supported by NSF
2007~2008	Travel Grant, IEEE S&P, supported by NSF, IARPA and ARO
2007~2009	Travel Grant, Graduate Division, UC Irvine
2006~2007	Travel Grant, CRA-W Grad Cohort Workshop, supported by Google and Microsoft
2005~2008	Dean's Fellowship, UC Irvine
2004	Tan Kah Kee Young Inventor's Award, Silver Medal, Tan Kah Kee Foundation

PROFESSIONAL EXPERIENCE

University of Michigan-Dearborn Dearborn, MI, USA
Assistant Professor of Computer and Information Science 09/2009 ~ present

University of California, Irvine Irvine, CA, USA
Graduate Student Researcher 09/ 2005 ~ 08/2009

IBM Almaden Research Center San Jose, CA, USA
Research Intern 06/2008 ~ 09/2008

Institute for Infocomm Research Singapore
Senior Research Engineer 06/2000 ~ 08/2005

TEACHING EXPERIENCE

CIS 387 Digital Forensics I	2011 Winter
CIS 405/505 Advanced Algorithm Design and Analysis	2011 Fall
CIS 437 Advanced Networks	2012 Winter
CIS 447/544 Introduction to Computer and Network Security	2009 Fall, 2010 Fall, 2011 Fall
CIS 546 Wireless Network Security and Privacy	2012 Winter

PUBLICATIONS

Book Chapters

1. **Di Ma** and Nitesh Saxena. Towards sensing-enabled RFID security and privacy. *Security and Trends in Wireless Identification and Sensing Platform Tags: Advancements in RFID.* Pp 65-88. IGI Global. Aug. 2012.
2. Robert Deng, Yongdong Wu, and **Di Ma**. Securing JPEG2000 code-streams. *Computer Security in the 21st Century* (ISBN: 0-387-24005-5). Springer, 2005.

Journal Papers

3. Bingsheng Zhang, Qin Zhan, Si Chen, Muyuan Li, Kui Ren, Cong Wang and **Di Ma**. PriWhisper: Enabling Keyless Secure Acoustic Communication for Smartphones. *IEEE Internet of Things Journal,* Vol. Issu. 99, pp. 1–13, January 2014.
4. Tzipora Halevi, Haoyu Li, **Di Ma**, Nitesh Saxena, Jonathan Voris, and Tuo Xiang. Context-Aware Defenses to RFID Unauthorized Reading and Relay Attacks. *IEEE Transactions on Emerging Topics in Computing (TETC)*, Vol. 1, Issu. 2, pp. 307–318, December 2013.
5. Yan Zhu, Gail-Joon Ahn, Hongxin Hu, **Di Ma**, and Shanbiao Wang. Role-based cryptosystem: A new cryptographic RBAC system based on role-key hierarchy. *IEEE Trans. on Information Forensics and Security (TIFS)*, Vol. 8, Issu. 12, pp. 2138-2153, December 2013.
6. **Di Ma**, Nitesh Saxena, Tuo Xiang, and Yan Zhu. Location-aware and safer cards: enhancing RFID security and privacy via location sensing. *IEEE Trans. on Distributed and Secure Computing (TDSC),* Vol. 10, Issu. 2, pp 57-69, March-April 2013.
7. Yan Zhu, Shanbiao Wang, Hongxin Hu, Gail-Joon Ahn, and **Di Ma**. Secure collaborative integrity verification for hybrid cloud environments. *International Journal of Cooperative Information Systems (IJCIS)*, Vol. 21, No. 3, pp 165-197, 2012.
8. Roberto Di Pietro, **Di Ma**, Claudio Soriente and Gene Tsudik. Self-healing in unattended wireless sensor networks. *ACM Tran. On Sensor Networks (ToSN),* vol. 9, no. 1, pp. 7:1--7:21, Nov. 2012.
9. **Di Ma** and Nitesh Saxena. A context-aware approach to defend against unauthorized reading and relay attacks in RFID systems. *Security and Communication Networks (2011)*. DOI: 10.1002/sec.404
10. **Di Ma** and Gene Tsudik. Security and privacy in emerging wireless networks. *IEEE Wireless Communications*, *Special Issue on Security and Privacy in Emerging Wireless Networks*, pp. 2~11, Oct. 2010.
11. **Di Ma,** Claudio Soriente and Gene Tsudik. New adversary and new threats in unattended sensor networks. *IEEE Network*, Mar/Apr 2009.
12. **Di Ma** and Gene Tsudik. A new approach to secure logging. *ACM Trans. on Storage (ToS)*, Vol. 5, Issu. 1, pp. 2:1--2:21, Mar. 2009.
13. Yongdong Wu, **Di Ma** and Robert H. Deng. Flexible access control to JPEG2000 image code-streams. *IEEE Trans. on Multimedia*, vol. 9, no. 6, pp. 1314-1324, Oct. 2007.
14. Robert H. Deng, **Di Ma**, Weizhong Shao and Yongdong Wu. Scalable trusted online dissemination of JPEG2000 images. *ACM/Springer Multimedia Systems*, vol. 11, pp. 60-67, Nov. 2005.
15. F. Lin, H.S. Seah, Z. Wu and **Di Ma**. Voxelization and fabrication of freeform models. *Virtual and Physical Prototyping*, vol. 2, no. 2, pp. 65-73, Jun. 2007.
16. **Di Ma**, F. Lin and C. K. Chua. Rapid prototyping applications in medicine, Part 1: NURBS-based volume modeling. *International Journal of Advanced Manufacturing Technology*, vol. 18, 2001.
17. **Di Ma**, F. Lin and C. K. Chua. Rapid prototyping applications in medicine, Part 2: STL generation

through volume modeling and iso-surface extraction. *International Journal of Advanced Manufacturing Technology*, vol. 18, 2001.

Conference Papers

18. Y. Zhu, **D. Ma**, and S. Wang. Enabling secure location-based services in mobile cloud computing. The 2nd Mobile Cloud Computing Workshop (MCC), in conjunction with ACM SIGCOMM, Hong Kong, China, Aug. 12-16, 2013.
19. Y. Zhu, **D. Ma**, and S. Wang. Efficient identity-based encryption without pairings and key escrow for mobile devices. The 8th International Conference on Wireless Algorithms, Systems, and Applications (WASA'13), Zhangjiajie, China, Aug. 7-10, 2013.
20. Y. Zhu, **D. Ma**, C. Hu, and D. Huang. 2013. How to use attribute-based encryption to implement role-based access control in the cloud. *ACM international workshop on Security in cloud computing (Cloud Computing '13)*, pp 33-40. In conjunction with ACM Symposium on Information, Computer and Communications Security (AsiaCCS), Hangzhou, China, May 7-10, 2013.
21. **D. Ma**, Y. Zhu, and M. Yu. End-to-end aggregate authentication of time-series data. *ACM Workshop on Asia Public-Key Cryptography (AsiaPKC'13)*, pp 51-56. In conjunction with ACM Symposium on Inforamtion, Computer and Communications Security (AsiaCCS), Hangzhou, China, May 7-10, 2013.
22. H. Li, **D. Ma**, N. Saxena, B. Shrestha, and Yan Zhu. Tap-Wave-Rub: Lightweight Malware Prevention for Smartphones using Intuitive Human Gestures. *ACM Conference on Wireless Network Security (WiSec)*. Budapest, Hungary. April 2013.
23. Y. Zhu, S. Wang, **D. Ma**, H. Hu and G. Ahn. Secure and Efficient Constructions of Hash, MAC and PRF for Mobile Devices. *IEEE Global Communications Conference, Exhibition and Industry Forum (GlobeCom)*, Dec. 2012.
24. T. Halevi, **D. Ma**, N. Saxena and T. Xiang. Secure Proximity Detection for NFC Devices based on Ambient Sensor Data*. European Symposium on Research in Computer Security (ESORICS),* Sept. 2012.
25. Y. Zhu, **D. Ma**, and S. Wang. Secure Data Retrieval of Outsourced Data with Complex Query Support. ICDCS Workshop on Security and Privacy in Cloud Computing (ICDCS-SPCC), Jun. 2012.
26. **D. Ma**, A. K. Prasad, N. Saxena, and T. Xiang.Location-Aware and Safe Card: Enhancing RFID Security and Privacy via Location Sensing. *ACM Conference on Wireless Network Security (WiSec)*. Tucson, Arizona. April 2012
27. T. Halevi, S. Lin, **D. Ma**, A. K. Prasad, N. Saxena, J. Voris, and T. Xiang. Sensing-enabled Defenses to RFID Unauthorized Reading and Relay Attacks without Changing the Usage Model. *International Conference on Pervasive Computing and Communications (PerCom)*, March 2012.
28. **Di Ma** and Claudio Soriente. Building trust for λ -congenial secret groups. *6th International Conference on Broadband and Wireless Computing, Communication and Applications.* Barcelona, Spain. Oct. 2011.
29. **Di Ma** and Anudath K Prasad. A context-aware approach for enhanced security and privacy in RFID electronic toll collection systems. *5th Workshop on Wireless Mesh and Ad Hoc Networks (WiMAN), in conjunction with IEEE International Conference on Computer Communication Networks (ICCCN)*, Hawaii, Aug. 2011
30. **Di Ma** and Hongxia Jin. Content usage tracking in superdistribution. *IEEE Consumer Communications and Networking Conference*, Las Vegas, Jan. 9-12, 2011.
31. **Di Ma** and Gene Tsudik. IRRES: Intrusion Resilient Remote Email Storage. *First ICDCS Workshop on Security and Privacy in Cloud Computing*, Gonoa, Italy, 2010
32. Rex Chen, **Di Ma** and Amelia Regan. TARI: Meeting delay requirements in VANETs with efficient authentication and revocation. *Proc. International Conference on Wireless Access in Vehicular Environments (WAVE)*, 2009.
33. **Di Ma** and Gene Tsudik. DISH: distributed self-healing in unattended wireless sensor networks. *Proc. 10th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'08)*, Detroit, MI, Nov. 2008.
34. Roberto Di Pietro, **Di Ma**, Claudio Soriente and Gene Tsudik. POSH: Proactive co-operative self-healing in unattended wireless sensor networks. *Proc. IEEE 27th International Symposium on Reliable*

Distributed Systems (SRDS'08), Napoli, Italy, Oct. 2008.

35. **Di Ma** and Gene Tsudik. A new approach to secure logging. *Proc. 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSEC'08)*, London, UK, Jul. 2008.
36. **Di Ma.** Practical forward secure sequential aggregate signatures. *Proc. ACM Symposium on Information, Computer and Communications Security (ASIACCS'08)*, Tokyo, Japan, Mar. 2008.
37. **Di Ma** and Gene Tsudik. Forward-secure sequential aggregate authentication. *Proc. IEEE Symposium on Security and Privacy (S&P'07)*, Oakland, CA, May 2007.
38. **Di Ma**, "Securing feedback service for wireless sensor networks. *Proc. 3rd Information Security Practice and Experience Conference (ISPEC'07)*, Hong Kong, China, May 2007.
39. **Di Ma**, Robert H. Deng, Hweehwa Pang and Jianying Zhou. Authenticating query results in data publishing. *Proc. 7th International Conference on Information and Communications Security (ICICS'05)*, LNCS 3783, pp. 376-388. Beijing, China, Dec. 2005.
40. **Di Ma**, Robert H. Deng, Yongdong Wu and Tieyan Li. Dynamic access control for multi-privileged group communications. *Proc. 6th International Conference on Information and Communications Security (ICICS'04)*, LNCS 3269, pp. 508-519, Malaga, Spain, Oct. 2004.
41. Tieyan Li, Yongdong Wu, **Di Ma**, Huafei Zhu and Robert H. Deng. Flexible verification of MPEG-4 stream in peer-to-peer CDN. *Proc. 6th International Conference on Information and Communications Security (ICICS'04)*, LNCS 3269, pp. 79-91, Malaga, Spain, Oct. 2004.
42. Yongdong Wu, **Di Ma**, Tieyan Li and Robert H. Deng. Classify encrypted data in wireless sensor networks. *Proc. IEEE Vehicular Technology Conference*, Los Angels, CA, Sep. 2004.
43. Yongdong Wu, **Di Ma** and Robert H. Deng. Progressive protection of JPEG2000 code-streams. *Proc. IEEE International Conference on Image Processing (ICIP'04)*, pp. 3439-3442, Singapore, Oct. 2004.
44. Hongjun Wu and **Di Ma**. Efficient and secure encryption schemes for JPEG2000. *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2004)*, Montreal, Canada, May 2004.
45. Robert H. Deng, Yongdong Wu and **Di Ma**. Securing JPEG2000 code-streams. *Proc. International Workshop on Advanced Developments in Software and Systems Security*, Dec. 2003.
46. Yongdong Wu, **Di Ma** and Changsheng Xu. Efficient object-based stream authentication. *Proc. 3rd International Conference on Cryptology in India (IndoCrypto 2002)*, LNCS 2551, pp. 354-367, Hyderabad, India, Dec. 2003.
47. **Di Ma**, F. Lin and C. K. Chua. Volume modeling for rapid prototyping. *Proc. 10th Annual Solid Freeform Fabrication Conference*, Austin, TX, Aug. 1999.

Patents

1. (granted) Yongdong Wu, Xiaofeng Wei, and **Di Ma**. Method and system for deterrence of unauthorized reuse of display content. WO 2004/019152, US 2006/0110004 A.
2. Di Ma and Hongxia Jin. Content Usage Tracking in Superdistribution. US Patent Pending, IBM Docket No. ARC920090088US1, Filed by IBM Almaden Research Center, 2010.

Contributions to Standards (ISO/IEC 15444-8, selected**)**

1. Yongyong Wu, **Di Ma**, Robert Deng. ImTrust: design and implementation. ISO/IEC JTC 1/SC 29/WG1/N3075.
2. **Di Ma**, Yongdong Wu, Robert Deng, ImAccess: design and implementation. ISO/IEC JTC 1/SC 29/WG1/N3312.
3. Junichi Hayashi, Keiichi Iwamura, Yongdong Wu, **Di Ma**, Robert Deng. Progressive access to JPEG 2000 codestream. ISO/IEC JTC 1/SC 29/WG1/N3204.

Posters and Others

1. **Di Ma**, Claudio Soriente and Gene Tsudik. Self-defense in unattended wireless sensor networks. Poster paper, The 10th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'08), Detroit, MI, Nov. 2008.
2. **Di Ma** and Gene Tsudik. Forward secure sequential aggregate authentication. CRA-W Graduate Cohort

Workshop, San Francisco, 2007

3. **Di Ma**, Yongdong Wu and Robert Deng. Analysis of Canon encryption scheme," Communications in JPEG2000 Security group (JPSEC), Nov. 14, 2003.

PROFESSIONAL ACTIVITIES

Panelist or Judge:

- Proposal Review Panelist, NSF, 2011, 2012, 2013, 2014
- Proposal Review Panelist, Univ. of Michigan, 2014
- Fellowship Review Panelist, DoD, 2014
- Judge, Global Security Challenge – Midwest Regional Final, Sept. 21, 2010

Journal Editorial Board:

- Elsevier Journal of Computer Communications (COMCOM), Feb. 2014~ present
- Journal of Communications and Networks (JCN), Jul. 2014 ~ present
- Guest editor of two incoming special issue journals

Technical Program Committee Member:

- M2MSec'14: 1st International Workshop on Security and Privacy in Machine-to-Machine Communications, San Francisco, USA, Oct 29, 2014
- WISA'14: 15th International Conference on Information Security Applications, Juju Island, Korea, Aug 25-27, 2014
- WiSec'14: 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Oxford, UK, Jul 23-25, 2014
- ISPEC'14: 10th Information Security Practice and Experience Conference, Fuzhou, China, May 5-8, 2014
- GlobeCom 2013: IEEE Global Communications Conference, Miami, Florida, December 9-13, 2013.
- D-SPAN'13 – IEEE International Workshop on Data Security and Privacy in Wireless Networks, Madrid, Spain, June 4, 2013.
- ASIACCS'13-SCC – International Workshop on Security in Cloud Computing. Hanzhou, China. May 8-10, 2013.
- ASIACCS'13-SESP – International Workshop on Security in Embedded Systems and Smartphones. May 8-10, 2013.
- EUSPN'13 – International Conference on Emerging Ubiquitous Systems and Pervasive Networks. Niagara Falls, Ontario, Canada. Oct. 21-24, 2013.
- ICNC 2013 – IEEE International Conference on Computing, Networking and Communications. San Diego. Jan. 28-31, 2013.
- ICC'2013 – IEEE International Conference on Communications, Budapest, Hungary, Jun. 9-13, 2013
- ICCCN'13 – 22nd International Conference on Computer Communications and Networks, Nassau, Bahamas, Jul. 30-Aug. 2, 2013
- FC'2013 – Financial Cryptography and Data Security, Okinawa, Japan, Apr. 1-5, 2013
- ISPEC'13 – 9th Information Security Practice and Experience Conference, Lan Zhou, China, May 12-14, 2013
- ICNC'13 – International Conference on Computing, Networking and Communications. San Diego, Jan.28-31, 2013.
- ICICS'12 – International Conference on Information and Communications Security. Hong Kong. October 29-31, 2012.
- RFIDsec'12 Asia – Workshop on RFID and IoT Security. Taipei, Taiwan. Nov. 8-9, 2012.
- WiSec'2012 – 5rd ACM Conference on Security and Privacy in Wireless and Mobile Networks, Tucson,

Arizona, Apr. 16-18, 2012

- SPCC'12 – 3rd International Workshop on Security and Privacy in Cloud Computing, in conjunction with ICDCS 2012, Macau, China, June 18-21, 2012.
- Milcom'12 – 2012 Military Communications Conference. . Orlando, Florida. October 29 – November 1, 2012.
- MUSIC 2012 – The 2012 FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing, Ubiquitous Computing track. Vancouver, Canada, June 2012
- CCNC 2012 - The 9th Annual IEEE Consumer Communications and Networking Conference - Security and Content Protection, Las Vegas, January, 2012.
- CANS 2011 – The 5th International Conference on Cryptology And Network Security, Sanya, China, December 2011
- EUC 2011: The 9th IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Melbourne, Australia, October 2011
- GlobeCom 2011: IEEE Global Communications Conference, Houston, Texas, December 2011
- VTC2011-Fall: IEEE 74th Vehicular Technology Conference, San Francisco, September 2011
- WiMAN'11: 5th Workshop on Wireless Mesh and Ad Hoc Networks (WiMAN), in conjunction with IEEE International Conference on Computer Communication Networks (ICCCN), Hawaii, Aug. 2011.
- SPCC'11 – 2nd International Workshop on Security and Privacy in Cloud Computing, in conjunction with ICDCS 2011, Minneapolis, Minnesota, USA, June 20-24, 2011.
- ACNS'11 – 9th International Conference on Applied Cryptography and Network Security, Nerja, Spain, June 7-10, 2011.
- WiSec'2011 – 3rd ACM Conference on Wireless Network Security, Hamburg, Germany, June 14-17, 2011
- CCNC'2011 - The 8th Annual IEEE Consumer Communications and Networking Conference - Security and Content Protection, Las Vegas, January, 2011.
- ISC 2010: 13th Information Security Conference, Boca Raton, Florida, October 2010
- CCSW 2010: ACM Cloud Computing Security Workshop, in conjunction with ACM CCS 2010, Chicago, Illinois, October 2010
- MINES 2010: IEEE International Conference on Multimedia Information NEtworking and Security, Nanjing, China, November 2010
- VTC2010-Fall: IEEE 72nd Vehicular Technology Conference, Ottawa, Canada, September 2010
- GlobeCom 2010: IEEE Global Communications Conference, Miami, Florida, December 2010
- WAVE2009: IEEE International Conference on Wireless Access in Vehicular Environments, Shanghai, China, December 2009
- UbiSafe-09: IEEE International Symposium on Ubisafe Computing, Chengdu, China, December 2009

External Conference Reviewer: IWSEC 2010, CANS 2009, IFIP SEC 2009, ASIACCS 2007~2009, ACSAC 2008, ACM DRM 2008, ICICS 2008, ICNP 2008~2009, EuroPKI 2008, PET 2008, IEEE S&P 2008, ACM CCS 2007, HealthNet 2007, SCN 2006, CISC 2006, ISCAS 2006

Journal Reviewer: VLDB Journal, ACM Trans. on Information and System Security, ACM Trans. on Sensor Networks, ACM/Springer Multimedia Systems, IEEE Journal on Selected Areas in Communications, IEEE Trans. on Information Forensics and Security, IEEE Trans. Reliability, IEEE Wireless Communications, IEEE Trans. on Smart Grid, IEEE Communication Letters, IET Information Security, EURASIP Journal on Information Security, EURASIP Journal on Wireless Communications and Networking, EURASIP Journal on Signal Processing, Wiley Wireless Communications and Mobile Computing, Wiley's Security and Communication Networks, Journal of Communication System, Journal of Systems and Software, Ad Hoc Networks, International Journal of Information Systems, Elsevier Journal of Computer Communications, Elsevier Journal of Computers and Security

TALKS AND PRESENTATIONS

- (invited talk). Identity management in wireless networks. Future of Identity Workshop. London, UK. Apr. 9, 2013.
- (invited talk). Sensing-enabled RFID security and privacy. UMass-Lowell CIS Research Colloquium. Oct, 2012.
- Secure data retrieval of outsourced data with complex query support. ICDCS'12. Macau, China. June, 2012.
- Panel talk: Privacy in the smartphone age. NSF US-MidEast Workshop. Istanbul, Turkey. June, 2012.
- Location-aware and safe card: enhancing RFID security and privacy via location sensing. ACM WiSec'12. Tucson, Arizona. April 2012.
- Sensing-enabled RFID security and privacy. ECE Research Colloquium. April, 2012.
- Panel talk: Cryptographic approach for delegation and authorization in cloud computing. NSF Workshop on Security for Cloud Computing. Arlington, Virginia. March 2012.
- Sensing-enabled defenses to RFID unauthorized reading and relay attacks without changing the usage model. PerCom'12. Lugano, Switzerland. March 2012.
- A context-aware approach for enhanced security and privacy in RFID electronic toll collection systems. ICCCN'11. Maui, Hawaii. July 2011.
- Self-healing and automatic defense: security advances in sensor networks, RFID, and their combination. Technical Talk. Air Force Research Lab, WPAFB. July 2011.
- *(invited talk)* Intrusion Resilience for Unattended Sensor Networks. SRM University, India, June 2010
- IRRES: Intrusion Resilient Remote Email Storage. ICDCS-SPCC, Genoa, Italy, June 2010
- TARI: Meeting Delay Requirements in VANETs with Efficient Authentication and Revocation. CVPC's WAVE Seminar, March 11, 2010.
- *(invited talk)* New adversary and new threats: security in unattended wireless sensor networks, EECS, Syracuse University, May 2009
- *(invited talk)* New adversary and new threats: security in unattended wireless sensor networks, Informatics, Indiana University Bloomington, March 2009
- *(invited talk)* New adversary and new threats: security in unattended wireless sensor networks, CIS, Florida International University, March 2009
- *(invited talk)* New adversary and new threats: security in unattended wireless sensor networks, CIS, University of Michigan Dearborn, March 2009
- DISH: distributed self-healing in unattended wireless sensor networks, 10th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS'08), Detroit, MI, Nov. 2008
- On the unified revocation and tracing system. IBM Almaden Research Center, Sept. 2009
- A new approach to secure logging, 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSEC'08), London, UK, Jul. 2008
- Practical forward secure sequential aggregate signatures, *ACM Symposium on Information, Computer and Communications Security (ASIACCS'08)*, Tokyo, Japan, March 2008
- Forward-secure sequential aggregate authentication, IEEE Symposium on Security and Privacy (S&P'07), Oakland, CA, May 2007.
- Providing secure feedback service for wireless sensor networks, 3rd Information Security Practice and Experience Conference (ISPEC'07), Hong Kong, China, May 2007.
- ImAccess: a method for JPEG 2000 access control, 29th ISO/IEC JTC 1/SC 29/WG1 meeting, Seoul, Mar. 2003