

CURRICULUM VITAE

NAME: Huaxiong Wang

DATE OF BIRTH: 15th January 1965

NATIONALITY: Australian

PRESENT POSITION: Senior Lecturer
Department of Computing
Division of Information and Communication Sciences
Macquarie University

ADDRESS: Department of Computing
Division of Information and Communication Sciences
Macquarie University
Sydney, NSW 2109, Australia
Email: hwang@ics.mq.edu.au
Tel: +61-2-98509577
Fax: +61-2-98509551
Homepage: <http://www.comp.mq.edu.au/~hwang>

EDUCATION:

1996 PhD in Mathematics, University of Haifa, Israel
2001 PhD in Computer Science, University of Wollongong, Australia

PROFESSIONAL MEMBERSHIP: MIACR, MACM

RESEARCH AREAS: Cryptography, Information Security, Coding Theory and Theoretical Computer Science.

AWARDS:

- The inaugural Award for Best Research Contribution from the Computer Science Association of Australasia, 2004.

GRANTS:

- **Huaxiong Wang** and Jennifer Seberry and Chaoping Xing and Yvo Desmedt: Secure Multi-Party Computation, ARC discovery Project, \$390,000, 2006 – 2008.
- **Huaxiong Wang** and Chris Charnes: Private Information Retrieval, ARC discovery grant \$296,000, 2005 – 2007.
- **Huaxiong Wang**: Secure Key Agreement Protocols, MU Research Development Grant \$6,400, 2004.
- **Huaxiong Wang**: Security Services for Stream-Oriented and Multicast-Based Communication, ARC discovery grant \$100,000, 2003 – 2004.
- Josef Pieprzyk and **Huaxiong Wang**: Algebraic Analysis of Cryptosystems, ARC discovery grant \$225,000, 2003 – 2005.
- A. Nayak and **Huaxiong Wang** (with other 20 others): Intelligent Applications Through the Semantic Web, ARC Network Seeding Grant \$20,000, 2004.
- **Huaxiong Wang**: Efficient key management for secure multicast communication, Macquarie University New Staff Research Grant \$19,473, 2003.
- **Huaxiong Wang**: *XL* algorithm, Start-up Grant, Division of Information and Communication Sciences, Macquarie University, \$6,000, 2002.
- **Huaxiong Wang**: Key management for Re-keying, ARC Small Grant, University of Wollongong, \$5,200, 2001.
- Jennifer Seberry and **Huaxiong Wang** (with 4 others from Centre for Computer Security Research): Research Grant from UoW, \$30,000/per year, 2000 – 2001.

EMPLOYMENT:

- 1/2004 - Present: Senior Lecturer, Macquarie University, Australia
- 8/2005 - 2/2006: Senior Research Fellow, City University of Hong Kong, China.
- 1/2002 - 12/2003: Lecturer, Macquarie University, Australia
- 2/2001 - 1/2002: Lecturer, University of Wollongong, Australia
- 1/2000 - 2/2001: Research Fellow, University of Wollongong, Australia
- 3/1999 - 1/2000: Research Fellow, National University of Singapore, Singapore
- 10/1991 - 9/1992: Visiting Researcher, Kobe University, Japan

- 9/1990 - 9/1991: Lecturer, Fujian Normal University, China
- 9/1984 - 8/1990: Associate Lecturer, Fujian Normal University, China

TEACHING EXPERIENCE: I have taught the following subjects in recent years.

- *Advanced Information Security*, Macquarie University.
- *Cryptography and Information Security*, Macquarie University.
- *Optimisation* Macquarie University.
- *Software Engineering*, Macquarie University.
- *Advanced Computer Security*, University of Wollongong.
- *Designs and Analysis of Algorithms*, University of Wollongong.
- *Computer Security*, University of Wollongong.

SUPERVISION

- Post Doctoral Fellows
 - Jin Yuan, Macquarie University, 2005 – present.
 - Ron Steinfeld, Macquarie University, 2003 – 2005 (with Josef Pieprzyk).
 - Hartono Kurnio, Macquarie University, 2004.
- PhD Students
 - Qingsong Ye, Macquarie University, (1st supervisor, co-supervision with Mehmet Orgun), July, 2005 –
 - Peishun Wang, Macquarie University, (1st supervisor, co-supervision with Josef Pieprzyk), February, 2005 –
 - Christophe Tartary, Macquarie University, (1st supervisor, co-supervision with Josef Pieprzyk), February 2004 –
 - Vijayakrishnan Pasapathinathan, Macquarie University, (2nd supervisor, co-supervision with Josef Pieprzyk), February 2006 –
 - Cameron McDonald, Macquarie University, (2nd supervisor, co-supervision with Josef Pieprzyk), February 2005 –

- Gaurav Gupta, Macquarie University, (2nd supervisor, co-supervision with Josef Pieprzyk), February 2005 –
 - Krystian Matusiewicz, Macquarie University, (2nd supervisor, co-supervision with Josef Pieprzyk), February 2004 –
 - Joe Cho, Macquarie University, in progress (2nd supervisor, co-supervision with Josef Pieprzyk), February 2003 –
 - Al-Ibrahim Mohamed, Macquarie University, (2nd supervisor, co-supervision with Josef Pieprzyk), completed 2004.
- Master Students (Research)
 - Vijayakrishnan Pasapathinathan, Macquarie University, (2nd supervisor, co-supervision with Josef Pieprzyk), completed August 2005
- Honours Students
 - Daniel Sutanty, Macquarie University, 2004
Thesis Title: *Threshold Cryptography*.
 - Jack Chen, Macquarie University, 2003
Thesis Title: *Design and Implementation of Micropayment Scheme*.
 - Joe Underwood, Macquarie University, 2002 (1st Class)
Thesis Title: *End-to-end Security for Voice over IP*.
- Mini Master Projects (by course)
 - Nguyen K. Do, Macquarie University, 2004
Thesis Title: *Biometric Authentication*
 - Jilong Li, Macquarie University, 2003
Thesis Title: *Visual Cryptography*.
- Summer Vacation Scholarship Projects
 - Donny Amalo, Macquarie University, 2004
Project Title: *Implementation of Perfect Hash Family*.
- Exchange Students
 - Shoulun Long, PhD (University of Science and Technology of China), Macquarie University, July - December, 2004.
 - Kristian Syversen, Master (the University of Oslo, Norway), Macquarie University, July - December, 2004.

PROFESSIONAL ACTIVITIES:

- Editorship
 - Editorial board of *Designs, Codes and Cryptography* (2006 –).
 - Editorial board of *Journal of Communications* (2006 –).
 - Editor of *Communications and Networks* (2004 –).
 - Invited Guest Editorial Board of *International Journal of Information and Computer Security (IJICS)*, Special Issue on *Cryptography in Computer System Security*, 2007/2008.
 - Invited Guest Editorial Board of *International Journal of Security and Networks (IJSN)*, Special Issue on *Cryptography in Networks*, 2005/2006.
 - Invited Guest Editor for *Communications of the CCISA*, Special issue on selected topics of cryptography and information security, 2003.
- Chair of International Conferences
 - Program Co-chair of *4th International Conference on Cryptology and Network Security (CANS05)*, Xiamen, China, December, 2005.
 - Program Co-chair of *9th Australasian Conference on Information Security and Privacy (ACISP04)*, Sydney, Australia, July, 2004.
 - Organising Chair of *Workshop on Cryptography and Computational Number Theory (CCNT'99)*, Singapore, 1999
- Steering Committee Member of International Conferences
 - International Conference on Cryptology and Network Security (2005 –)
- Program Committee Member of International Conferences
 - *The 3rd INFORMATION SECURITY PRACTICE and EXPERIENCE CONFERENCE (ISPEC 2007)*, Hong Kong, China, May 7 - 10, 2007
 - *ACM Symposium on Information, Computer and Communication Security (AsiaCCS'07)*, Singapore, March, 2007.
 - *The Australasian Information Security Workshop (Privacy Enhancing Technologies)*, Ballarat, Victoria, Australia, January 30 - February 2, 2007.
 - *The SKLOIS Conference on Information Security and Cryptology (CISC)*, Beijing, China, Nov 29 – Dec 1, 2006
 - *7th International Workshop on Information Security Applications (WISA 2006)*, Jeju Island, Korea, August 28-30, 2006.

- *International Conference on Wireless Algorithms, Systems, and Applications (WASA 2006)*, Xi'an, China, August 15-18, 2006.
- *The 2006 International Conference on Privacy, Security and Trust (PST 2006)*, Oshawa, Ontario, Canada, October, 2006.
- *International Workshop on Applied PKI (IWPA 2006)*, Qingdao, China, October, 2006.
- *Second International Workshop on Security in Ubiquitous Computing Systems (SecUbiq 06)*, Seoul Korea, August 1-4, 2006.
- *International Conference on Security and Cryptography (SECRYPT-2006)*, Setubal, PORTUGAL, August 7-10, 2006
- *Computer and Network Security Symposium – International Wireless Communications & Mobile Computing Conference (IWCMC 2006)*, Sheraton Wall Centre, Vancouver, Canada, July, 2006
- *Network Security and Information Assurance SYMPOSIUM (Part of Wireless-Com) 2006*,
- *Australasian Information Security Workshop 2006 (Network Security)*, Tasmania, Australia, January, 2006.
- *The Second International Workshop on Security in Networks and Distributed Systems (SNDS-06)*, Vienna, Austria, April, 2006.
- *ACM Symposium on Information, Computer and Communication Security (AsiaCCS'06)*, Taipei, Taiwan, March, 2006.
- *4th WESAS International Conference on Information Security, Communications and Computers (WSEAS05)*, Tenerife, Spain, December, 2005.
- *10th Australasian Conference on Information Security and Privacy (ACISP05)*, Brisbane, Australia, July, 2005.
- *Third Australasian Information Security Workshop (AISW 2005): Digital Rights Management* (in conjunction with Australasian Computer Science Week), Newcastle, Australia, 2005.
- *The 2005 IEEE International Conference on E-Technology, E-commerce and E-service (EEE-05)*, Hong Kong, China, 2005.
- *Advanced Workshop on Content Computing (AWCC)*, Zhenjiang, China, 2004.
- *International Conference on Security and Management*, USA, 2003,
- *Workshop on Coding, Cryptography and Combinatorics (CCC 2003)*, China, 2003.
- *3rd Information Security Workshop (ISW2000)*, Australia, 2000.
- *Advances in Cryptology – Asiacrypt'99*, Singapore, 1999.

- *4th Australasian Conference on Information Security and Privacy (ACISP'99)*, Australia, 1999.
- Referee of the international journals
 - ACM Transactions on Information Systems Security
 - Australasia Combinatorial Journal
 - Computers & Electrical Engineering
 - Designs, Codes and Cryptography
 - Finite Fields and Their Applications
 - IEEE Transactions on Computers
 - IEEE Transactions on Vehicular Technology
 - IEEE Communications Letters
 - Information and Computation
 - Information Processing Letters
 - International Journal of Computers and Applications
 - International Journal of Information Security
 - International Journal of Foundations of Computer Science
 - Information Science, An International Journal
 - International Journal of Web Services
 - Journal of Complexity
 - Journal of Computer Security
 - Journal of Communication and Networks
 - Journal of Mathematical Cryptology
 - Journal of Research and Practice in Information Technology
 - Journal of Systems and Software
 - SIAM Journal of Computing
 - Semigroup Forum
 - Theoretical Computer Science
 - The Computer Journal
- Theses Examiner
 - Terje Tollisen: Aspects of Micropayments, Master (Honour), University of Wollongong, 2001.

- Jun Qi Zhang: Oblivious Transfer Protocols for Securing Electronic Commerce, Master (Honour), University of Western Sydney, 2002.
- Weiliang Zhao: Security Techniques for Electronic Commerce Applications, Master (Honour), University of Western Sydney, 2002.
- YiQun Chen: Contributions to Privacy Preserving with Ring Signatures, Master (Honour), University of Wollongong, 2006.
- Organiser of Seminar Series
 - Centre for Advanced Computing – Algorithms and Cryptography, Macquarie University, (02/2002 – 12/2003).
 - School of Information Technology and Computer Science, University of Wollongong (01/2001 – 12/2001).
 - Centre for Computer Security Research, University of Wollongong (02/2000 – 01/2001).

INVITED TALKS

- Invited talks at the conferences/workshops
 - Invited speaker of the International Workshop of Advanced Developmen for Software and Systems Security, December, 5 - 7, 2003, Taipei, Taiwan.
 - Invited speaker of the International Workshop on Coding and Cryptogr September, 10 -14, 2001, National University of Singapore, Singapore.
 - Workshop of Cryptography and Computation Number Theory, 22- 26, November, 1999, Singapore.
- Invited talks at the seminars
 - University of Science and Technology of China, China (12/2003)
 - Tsinghua University, China (12/2003)
 - National Tsinghua University, Taiwan (12/2003)
 - University of Wollongong, Australia (07/2003)
 - University of Newcastle, Australia (04/2003).
 - Royal Holloway, University of London, UK (02/2002)
 - University of Science and Technology, Hong Kong (12/2002).
 - Xiamen University, China (12/2002, 12/2004, 12/2005).

- Fuzhou University, China (12/2004)
- Fujian Normal University, China (12/2002, 12/2004).
- National University of Singapore, Singapore (10/2000, 09/2001, 02/2002, 02/2003, 2/2005)
- Sydney University, Australia (05/1997).

VISITS

- City University of Hong Kong, China (04/2006)
- Zhong-San University, China (01/2006)
- HP Lab, China (11/2005)
- University of Science and Technology of China, China (12/2003)
- Tsinghua University, China (12/2003)
- National Tsinghua University, Taiwan (12/2003)
- Royal Holloway, University of London, UK (02/2002)
- University of Science and Technology, Hong Kong (12/2002, 12/2003, 08/2005).
- Xiamen University, China (12/2002, 12/2003, 12/2005).
- Fujian Normal University, China (12/2002, 12/2004, 12/2005).
- National University of Singapore, Singapore (10/2000, 09/2001, 2/2002, 2/2003, 2/2005)

CONFERENCES

- ACISP'06, th Australasian Conference on Information Security and Privacy, July 3-5, Melbourne, Australia.
- PKC'06, 9th international workshop on public-key cryptography, April, 2006, New York, USA.
- CANS'05, 4th International Conference on Cryptology and Network Security, December, 2005, Xiamen, Fujian, China.

- ITW'05, IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security (ITW 2005), October 16-19, 2005, Awaji, Yumebutai, Japan.
- COCOON'05, 11th International Computing and Combinatorics Conference, August 16-19, 2005, Kunming, Yunnan, China.
- ACISP'05, 10th Australasian Conference on Information Security and Privacy, July 4-6, 2005, Brisbane, Australia
- PKC'05, 8th international workshop on public-key cryptography, 23-26 January 2005, "Les Diablerets", Switzerland.
- AWCC04, Advanced Workshop on Content Computing, November, 2004, Zhenjiang, China.
- ACISP04, 9th Australasian Conference on Information Security and Privacy July 13 - 15, 2004, Sydney, Australia.
- ACSC'04, 27th Australasian Computer Science Conference, January 2004, Dunedin, New Zealand.
- WADIS'03, International Workshop on Advanced Developments in Software and Systems Security, December 2003, Taipei, Taiwan.
- Asiacrypt 2003, November/December 2003, Taipei, Taiwan.
- ECC'03, 7th Workshop on Elliptic Curve Cryptography, August 2003, Waterloo, Ontario, Canada.
- SAC'03, Tenth Annual Workshop on Selected Areas in Cryptography, August 2003, Ottawa, Canada.
- ACISP'03, Eighth Australasian Conference on Information Security and Privacy, July 2003, Wollongong, Australia.
- CT-RSA'03, Cryptographers' Track RSA Conference, April 2003, San Francisco, USA.
- ICISC'02, 5th International Conference on Information Security and Cryptology, November 2002, Seoul, Korea.
- ACISP'02, Seventh Australasian Conference on Information Security and Privacy, July 2002, Melbourne, Australia.
- Asiacrypt 2001, December 2001, Gold Coast, Queensland, Australia.

- AAEEC-14, the 14th Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, November 2001, Melbourne, Australia.
- Workshop on Coding and Cryptography, September 2001, National University of Singapore, Singapore.
- ACISP'01, 6th Australasian Conference on Information Security and Privacy, July 2001, Sydney, Australia.
- ISW'00, 3rd International Workshop on Information Security, December 2000, Wollongong, Australia.
- Indocrypt 2000, December 2000, Calcutta, India.
- CCS'00, 7th ACM Conference on Computer and Communication Security, November 2000, Athens, Greece.
- AWOCA'00, the Eleventh Australasian Workshop on Combinatorial Algorithms, July/August, 2003, Hunter Valley, Australia.
- ACISP'00, Fifth Australasian Conference on Information Security and Privacy, July 2000, Brisbane, Australia.
- ICISC'99, 2nd International Conference on Information Security and Cryptology, December 1999, Seoul, Korea
- CCNT'99, Workshop on Cryptography and Computational Number Theory, November 1999, Singapore.
- Asiacrypt '99, November 1999, Singapore.
- Crypto '99, August 1999, Santa Barbara, California, USA
- Asiacrypt '98, October 1998, Beijing, P.R.China
- ACISP'98, Third Australasian Conference on Information Security and Privacy Brisbane, June 1998, Brisbane, Australia.
- Second Australasian Conference on Information Security and Privacy, June, 1997, Sydney, Australia.

PUBLICATIONS:

Books, Edited Books and Book Chapter

1. (with Yvo Desmedt, Yi Mu, Yongqing Li) **Cryptology and Network Security** (edited), Proceedings of 4th International Conference, CANS 2005, Lecture Notes in Computer Science Vol. 3810, Springer 2005
2. (with Niederreiter H and Xing C) Function Fields over Finite Fields and Their Applications to Cryptography, in Book **Topics in Geometry, Coding Theory and Cryptography**, by Aenaldo Garcia and Henning Stichtenoth (editors), Springer to appear (47 pages)
3. (with J. Pieprzyk and V. Varadharajan) **Information Security and Privacy** (edited), Proceedings of 9th Australasian Conference, ACISP'04, Lecture Notes in Computer Science, Vol. 3108, 2004.
4. (with K. Y. Lam, I. Shparlinski and C. Xing) **Cryptography and Computational Number Theory** (edited), Proceedings of Workshop of Cryptography and Computational Number Theory, Birkhauser, 2001.
5. (with Z. Chen, Q. Chen and Y. Lin) **Linear Algebras**, Fujian Education Press, Vol.1(1991), Vol.2(1992).

Theses

1. **Some Semiring-Theoretic Aspects of Rational Events**. PhD thesis (Mathematics), University of Haifa, Israel, 1996.
2. **Unconditionally Secure Schemes for Distributed Authentication Systems**. PhD (Computer Science), University of Wollongong, Australia, 2001.

Journal Papers

1. (with Tartary C) *Efficient Multicast Stream Authentication for Fully Adversarial Network Model*, International Journal of Security and Networks (IJSN) - Special Issue on Cryptography in Networks, to appear.
2. (with Safavi-Naini R and Wong D) *Resilient LKH: Secure Multicast Key Distribution Schemes*, International Journal of Foundations of Computer Science, to appear.
3. (with Safavi-Naini R) *Secret Sharing Schemes with Partial Broadcast Channels*, Designs, Codes and Cryptography, to appear.
4. (with Long S, Pieprzyk J and Wong D) *Generalised Cumulative Arrays in Secret Sharing*, Designs, Codes and Cryptography, 40(2006), 191 - 209.

5. (with Steinfeld R and Pieprzyk J) *Lattice-Based Threshold-Changeability for Standard CRT Secret-Sharing Schemes*. Finite Fields and Their Applications, to appear.
6. (with Martin K, Safavi-Naini R and Wild P) *Distributing the encryption and decryption of a block cipher*. Designs, Codes and Cryptography, 36(2005), 263-287.
7. (with Pieprzyk J) *Shared generation of pseudo-random functions*. Journal of Complexity, 20(2004), 458 - 472.
8. (with Xing C) *Algebraic curves over finite fields and applications to combinatorial cryptography*. Communications of the CCISA, Special issue on selected topics of cryptography and information security, Vol.9, No. 4, 2003, 64-77.
9. (with Xing C and Safavi-Naini R) *Linear Authentication Codes: Bounds and Constructions*. IEEE Trans. on Info. Theory, Vol. 49, No. 4, 2003, 866-872.
10. (with Safavi-Naini R) *Bounds and Constructions for Shared generation of authenticators*, International Journal of Computer Mathematics, Vol. 79, No. 12, 2002, 1285-1301.
11. (with Safavi-Naini R, Susilo W) *Fail-stop signature for long messages*, Journal of Information Science and Engineering, Vol 17, 2001, 879-898.
12. (with Safavi-Naini R) *Efficient Authentication for Group Communication*. Theoretical Computer Science, Vol. 269, 1-2, 2001, 1-21.
13. (with Xing C) *Explicit Constructions of Perfect Hash Families from Algebraic Curve over Finite Fields*. Journal of Combinatorial Theory, Series A, Vol.93, 2001, 112-124.
14. (with Desmedt Y, Safavi-Naini R, Batten L M, Charnes C and Pieprzyk J) *Broadcast Anti-jamming Systems*. Computer Networks, Vol. 35, No. 2-3, 2001, 223-236.
15. (with Xing C and Lam K Y) *Constructions of Authentication Codes from Algebraic Curves over Finite Fields*. IEEE Trans. on Info.Theory, Vol.46, 2000, 886-892.
16. (with K. M. Martin and Safavi-Naini R) *Bounds and Techniques for Efficient Redistribution of Secret Shares to New Access Structures*, The Computer Journal, Vol.42, No.8, 1999, 638-649.
17. (with K. M. Martin, J. Pieprzyk and R. Safavi-Naini) *Changing thresholds in the absence of secure channels*, Australian Computer Journal, Vol. 31, No.2, 1999, 34-43.
18. (with R. Safavi-Naini) *Multireceiver Authentication Codes: Model, Bounds, Constructions and Extensions*, Information and Computation, Vol. 151, No. 1/2, 1999, 148-172.

19. *On Syntactic Nuclei of Rational Languages*, Information Processing Letters, Vol67, No.5,1998, 221-226.
20. *On rational Languages and Rational Series*, Theoretical Computer Science. Vol. 205, No. 1-2, 1998, 329-336.
21. *On Characters of Semirings*, Houston J. Math. Vol 23, No. 3, 1997, 391-405.
22. (with J. Golan) *On Embedding in Complete Semirings*, Communications in Algebra, 24(9), 1996, 2945-2962.
23. *Injective Hulls of Semimodules over Additively-idempotent Semirings*, Semigroup Forum, 48, 1994, 377-379.
24. (with C. S. Hoo) *Extensions of BCI, BCK and MV-algebras*, Southeast Asian Bull. Math. 18, 1994, 47-53.
25. (with M. Takahashi) *Injective Semimodules over 2-semirings* ,Kobe J. Math. 10, 1993, 57-70.
26. (with Chen Z) *Closed Ideals and Congruences on BCI algebras*, Kobe J. Math. 8, 1991, 1-9.
27. (with Z. Chen) *On Simple BCI algebras*, Math. Japon. 36,4, 1991, 627-633.
28. (with Z. Chen) *On Ideals in BCI algebras*, Math.Japon. 36,3, 1991,497-501.
29. *Injective in BCI algebras*, Math. Japon. 35, 4, 1990, 797-798.
30. (with M. Takahashi) *On Epimorphisms of Semimodules*, Kobe J. Math. 6, 1989, 287-289.
31. (with Z. Chen) *Some Universal Properties of BCI-algebras*, Kobe J. Math. Vol.6 No.1, 1989, 43-48.
32. *A Note on Endomorphism Semirings of Semimodules*, Kobe J. Math. Vol.5, No.1, 1988, 155-160.

Refereed Conference Papers

1. (with Tartary C) *Rateless Codes for the Multicast Stream Authentication Problem*, The 1st International Workshop on Security (IWSEC2006), Lecture Notes in Computer Science, to appear.

2. (with Desmedt Y, Pieprzyk J and Steinfeld R) *A Non-Malleable Group Key Exchange Protocol Robust Against Active Insiders*, ISC2006, Lecture Notes in Computer Science, to appear.
3. (with Yang G and Wong D and Deng X) *Anonymous Signature Schemes*. International Workshop on Practice and Theory in Public Key Cryptography (PKC'06). Lecture Notes in Computer Science, Vol. 3958, 2006, 347 - 343.
4. (with Steinfeld R and Pieprzyk J) *Higher Order Universal One-Way Hash Functions from the Subset Sum Assumption*. International Workshop on Practice and Theory in Public Key Cryptography (PKC'06). Lecture Notes in Computer Science, Vol. 3958, 2006, 157 - 173.
5. (with Gupta G and Pieprzyk J) *An attack-localizing watermarking scheme for natural language documents*. Proceedings of the ACM Symposium on InformAtion, Computer and Communications Security(ASIACCS'06) ACM Press, 2006, 157 - 165.
6. (with Pasupathinathan V, Pieprzyk J, Cho J Y) *Formal Analysis of Card-based Payment Systems in Mobile devices*. In proceedings of 4th Australasian Information Security Workshop (AISW-NetSec 2006), Hobart, Tasmania, Jan 2006. Conferences in Research and Practice in Information Technology (CRIPT), Vol, 54.
7. (with Wu B, Lam K-Y, Chung S L) *Secure Construction of Virtual Organizations in Grid Computing Systems*. Proceedings of Internet and Network Economics, First International Workshop, WINE 2005, Lecture Notes in Computer Science 3828, 2005, 959-968.
8. (with Tartary C) *Efficient Multicast Stream Authentication for the Fully Adversarial Network Model*. The 6th International Workshop on Information Security Applications (WISA 2005), Lecture Notes in Computer Science, Vol. 3786, 2005, 108 - 125
9. (with Desmedt Y, Wang Y and Safavi-Naini R) *Radio Networks with Reliable Communication*. *Cocoon 2005, 11th Annual International Computing and Combinatorics Conference*, Lecture Notes in Computer Science, Vol. 3595, 2005, 156 - 166.
10. (with Pasupathinathan V and Pieprzyk J) *Privacy Enhanced Electronic Cheque System*. 7th IEEE International Conference on E-Commerce Technology, IEEE Computer Science, 431-434.
11. (with Steinfeld R, Contini S and Pieprzyk J) *Converse Results to the Wiener Attack on RSA*. International Workshop on Practice and Theory in Public Key Cryptography (PKC'05). Lecture Notes in Computer Science, Vol. 3386, 2005, 184 - 198.

12. (with Kurnio H, Pieprzyk J and Gaj K) *Securing Multicast Groups in Ad Hoc Networks*. Advanced Workshop on Content Computing (AWCC'04), Zhenjiang, China, 2004. Lecture Notes in Computer Science, Vol. 3309, 2004, 194 - 207.
13. (with Steinfeld R and Pieprzyk J) *Lattice-Based Threshold-Changeability for Standard Shamir Secret-Sharing Schemes*. 10th International Conference on the Theory and Application of Cryptology and Information Security, Asiacrypt'04. Lecture Notes in Computer Science, Vol. 3329, 2004, 170 - 186.
14. (with Steinfeld R and Pieprzyk J) *Efficient extension of standard Schnorr/RSA signature into universal designated-verifier*. International Workshop on Practice and Theory in Public Key Cryptography (PKC'04). Lecture Notes in Computer Science, Vol. 2942, 2004, 86 - 100.
15. (with Safavi-Naini R) *Resilient LKH: secure multicast key distribution schemes* (invited), Proceedings in 2003 International Workshop of Advanced Developments in Software and Systems Security (WADIS 2003), 2003, 44-50.
16. (with Pieprzyk J and Xing C) *Multiple-Time Signature Schemes Secure against Adaptive Chosen Message Attacks*, 10th Workshop on Selected Areas in Cryptography (SAC'03). Lecture Notes in Computer Science, Vol. 3006, 2004, 88 - 100.
17. (with Pieprzyk J) *Malleability Attacks on Multi-party Key Agreement Protocols*. Coding, Cryptography and Combinatorics (CCC 2003), Birkhäuser, Basel, 2004, 277 - 288.
18. (with Pieprzyk J) *Efficient one-time proxy signatures*, 9th International Conference on the Theory and Application of Cryptology and Information Security, Asiacrypt'03. Lecture Notes in Computer Science, Vol 2894, 2003, 507 - 522.
19. (with Steinfeld R, Bull L and Pieprzyk J) *Universal designated-verifier signatures*, 9th International Conference on the Theory and Application of Cryptology and Information Security, Asiacrypt'03. Lecture Notes in Computer Science, Vol 2894, 2003, 523 - 542.
20. (with Pieprzyk J) *Shared generation of pseudo-random function with cumulative maps*, CT-RSA'03. Lecture Notes in Computer Science Vol. 2612, 2003, 281-294.
21. (with Martin K, Pieprzyk J, Safavi-Naini R and Wild P) *Threshold MACs*. The 5th international conference on information security and cryptology, ICISC'02. Lecture Notes in Computer Science, Vol. 2587, 2003, 237-252.
22. (with Kurnio H, McAven L and Safavi-Naini R) *A Dynamic Group Key Distribution Scheme with Flexible User Join*. The 5th international conference on information security and cryptology, ICISC'02. Lecture Notes in Computer Science, Vol. 2587, 2003, 478-496, 2003.

23. (with Kurnio H and Safavi-Naini R) *A group key distribution scheme with decentralised user join*. Third Conference on Security in Communication Networks '02 September 12-13, 2002 Amalfi, Italy. Lecture Notes in Computer Science, Vol. 2576, 2003, 146-163.
24. (with Pieprzyk J) *A Combinatorial Approach to Anonymous Membership Broadcast*, Cocoon'2002, 8th Annual International Computing and Combinatorics Conference, Lecture Notes in Computer Science, Vol. 2387, 2002, 162 – 170.
25. (with Kurnio H and Safavi-Naini R) *A Secure Re-keying Scheme with Key Recovery Property*, 7th Australasian Conference on Information Security and Privacy, ACISP 2002, Lecture Notes in Computer Science, Vol. 2384, 2002, 40 – 55.
26. (with Desmedt Y and Safavi-Naini R) *Redistribution of a mechanical secret's shares*, Financial Cryptography'02, Lecture Notes in Computer Science, Vol. 2357, 2002, 238–252.
27. (with H. Kurnio and R. Safavi-Naini) *Efficient Revocation Schemes for Secure Multicast*, International Conference on Information Security and Cryptology–ICISC'01, Lecture Notes in Computer Science, Vol. 2288, 2002, 160-177.
28. (with Song B, and Seberry J) *A new cryptanalysis method using the distribution characteristics of substitution distance*, International Conference on Information Security and Cryptology 2001, Lecture Notes in Computer Science, Vol. 2288, 2002, 18-31.
29. (with Safavi-Naini R and Xing C) *Linear Authentication Codes: Bounds and Constructions*, Indocrypt'01, Lecture Notes in Computer Science, Vol. 2247, 2001, 127–135.
30. (With R. Safavi-Naini and W. Susilo) *How to construct fail-stop confirmer signature schemes*, 6th Australasian Conference on Information Security and Privacy, ACISP 2001, Lecture Notes in Computer Science, **2119**(2001), 435-444.
31. (with Y. Desmedt, M. Burmester and R. Safavi-Naini) *Threshold Things That Thinks (T^4): security requirements to cope with theft of handheld/handless internet devices*, The Symposium on Requirements Engineering for Information Security, West Lafayette, Indiana, USA, 2001.
32. (with R. Safavi-Naini) *New Constructions of secure multicast re-keying schemes using perfect hash families*, 7th ACM Conference on Computer and Communication Security, ACM Press, 2000, 228-234.
33. (with R. Safavi-Naini and W. Susilo) *Fail-Stop Signature for long messages*, Indocrypt'00, Lecture Notes in Computer Science, **1977**(2000), 165-177.

34. (with R. Safavi-Naini) *Bounds and Constructions for Shared generation of authenticators*, Proceedings of the Eleventh Australasian Workshop on Combinatorial Algorithms, AWOCA 2000, 93–110.
35. (with Kurnio H, and Safavi-Naini R and W. Susilo) *Key Management for Secure Multicast with Dynamic Controllers*, Fifth Australasian Conference on Information Security and Privacy, ACISP 2000, Lecture Notes in Computer Science 1841 (2000) 178–190.
36. (with Lam K Y, Xiao G-Z and Zhao H) *On Multiplicative Secret Sharing Schemes*, Fifth Australasian Conference on Information Security and Privacy, ACISP 2000, Lecture Notes in Computer Science 1841 (2000) 241–251.
37. (with Safavi-Naini R) *Robust Secret Sharing Schemes over Abelian Group Z_m* , Cryptography and Combinatorial Number Theory (CCNT '99), Progress in Computer Science and Applied Logic, Vol. 20, Birkhauser, 2001, 244-257.
38. (with Safavi-Naini R) *Broadcast authentication in group communication*, ASIACRYPT'99, Lecture Notes in Computer Science, Vol. 1716, 1999, 399-41.
39. (with Y. Desmedt, R. Safavi-Naini, C. Chris and J. Pieprzyk, *Broadcast Anti-jamming Systems*, ICON '99, IEEE International Conference on Networks, IEEE Computer Society, 1999, 349-355.
40. (with Martin K M, Pieprzyk J and Safavi-Naini R) *Changing thresholds in the absence of secure channels*, Proceedings of Information Security and Privacy Conference, Lecture Notes in Computer Science, Vol. 1578, Springer-Verlag, 177-191, 1999.
41. (with Safavi-Naini R and Lam K Y) *A new approach to robust threshold RSA signature* Proceedings of Information Security and Cryptology–ICISC'99, Lecture Notes in Computer Science, **1787**(2000), 184-196.
42. (with Safavi-Naini R) *New Results on Multireceiver Authentication Codes* In Advances in Cryptology - EUROCRYPT '98, Lecture Notes in Computer Science **1403**, 527-541, 1998.
43. (with Safavi-Naini R) *Bounds and Constructions for Multireceiver Authentication Codes* In 'Advances in Cryptology - ASIACRYPT '98', Lecture Notes in Comp. Sci. **1514**(1998), 242-256.
44. (with Ghodosi H., Pieprzyk J. and Safavi-Naini R) *On Construction of Cumulative Secret Sharing Schemes*, In Proceedings of ACISP'98 (Australian Conference on Information Security and Privacy), Lecture Notes in Computer Science, **1438**, 378-390, 1998.