

RESUME

4 December 2024

1 Personal

Name : Robert Deng Huijie
Nationality : Singapore
Telephone : Office: +65 6828-0920; Mobile: +65 9752-3057
E-mail : robertdeng@smu.edu.sg

2 Education

- 01/1984 – 12/1985: Illinois Institute of Technology, Chicago, USA, Ph.D
- 01/1983 – 12/1983: Illinois Institute of Technology, Chicago, USA, M.Sc
- 03/1978 – 12/1981: National University of Defence Technology, China, B.Eng, Outstanding Graduate

3 Present and Past Appointments

- 07/2018 – present, Deputy Dean for Faculty & Research, School of Computing & Information Systems, Singapore Management University
- 04/2019 – 12/2023, Programme Director of National Satellite of Excellence in Mobile Systems Security and Cloud Security, Singapore National Research Foundation National Cybersecurity Research Programme
- 09/2016 – 06/2018, Dean, Postgraduate Research Programme, Singapore Management University
- 03/2017 – 03/2025, AXA Chair Professor of Cybersecurity, AXA Research Fund
- 01/2015 – 12/2023, Director of Secure Mobile Centre, Singapore Management University
- 07/2005 – 06/2014, Professor, Director of SIS Research Centre, Associate Dean for Faculty & Research, School of Information Systems, Singapore Management University
- 07/2004 – 06/2015, Professor, Head of Information Security & Trust Cluster, School of Information Systems, Singapore Management University
- 04/1997 – 07/2004: Principal Scientist and founding Head of Infocomm Security Department, A*Star Institute for Infocomm Research (previously called Kent Ridge Digital Labs and Laboratories for Information Technology)
- 07/1994 – 03/1997: Senior Research Staff Member and Leader of Information Security Group, Institute of Systems Science, National University of Singapore
- 07/1991 – 06/1994: Senior Lecturer, Department of Electrical and Computer Engineering, National University of Singapore
- 07/1987 – 06/1991: Research Staff Member and Project Leader of Communications Group, Institute of Systems Science, National University of Singapore
- 01/1986 – 06/1987: Postdoctoral Research Associate, University of Notre Dame, USA
- 01/1984 – 12/1985: Research Assistant, Illinois Institute of Technology, Chicago, USA
- 01/1982 – 12/1982: Teaching Assistant, Beijing University of Aeronautics & Astronautics, Beijing, China

4 Awards and Recognitions

- Ranked among top 1% of scientists in the world by Stanford University since 2020
- Outstanding Paper Award, the 21st IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2022), 9-11 December 2022
- Best Paper Award, the 5th IEEE Conference on Dependable and Secure Computing (IEEE DSC 2022), Edinburgh, UK, 22-24 June 2022
- Huawei Technology Cooperation Excellence Award, December 2020
- Best Paper Award, the 26th IEEE International Conference on Parallel and Distributed Systems (ICPADS 2020), Hong Kong, 2 – 3 December 2020
- Best Paper Award, the 25th European Symposium on Research in Computer Security (ESORICS) 2020, Guildford, United Kingdom, 14 - 18 September 2020
- The Public Administration Medal (Silver), Singapore National Day Awards 2020, 9 August 2020
- Fellow of the Academy of Engineering Singapore, June 2019
- 2017 Best Journal Paper, IEEE Communications Society, Big Data Technical Committee, 2017
- Huawei Distinguished Collaboration Project Award, August 2016
- Fellow of the IEEE, January 2016
- Distinguished Lecturer, the Croucher Foundation Advanced Study Institute, City University of Hong Kong, 2014
- Distinguished Paper Award, the 19th Annual Network & Distributed System Security Symposium (NDSS2012), February 2012
- Best Paper Award, the 13th Joint IFIP TC6 & TC11 Conference on Communications and Multimedia Security (CMS2012), September 2012
- Asia-Pacific Information Security Leadership Achievements (ISLA) Community Service Star and Showcased Senior Information Security Professional, International Information Systems Security Certification ((ISC)²), USA, July 2010
- ACM Recognition of Service Award, 2007
- Lee Kuan Yew Fellow for Research Excellence, Singapore Management University, 2005
- Role Model for the Category of Principal Research Staff Member, Laboratories for Information Technology, 2002
- University Outstanding Researcher Award, National University of Singapore, November 1999
- KRDL Excellence Award, Kent Ridge Digital Labs, March 1999
- KRDL Achievement Award, Kent Ridge Digital Labs, June 1998
- ISS Meritorious Award, Institute of Systems Science, National University of Singapore, October 1990
- US NASA Research Fellowship, 1986-1987
- First Prize of the University Physics Contest, National University of Defence Technology, China, May 1980

5 Services

SMU Services

- Member of University Research Evaluation Committee (UREC) (2022 – 2025)
- Member of External Academic Review (EAR) Panel for the School of Law (SOL) (2019)
- Member of SMU Named Award Committee (2018 – present)
- Chair-elect (2010 – 2011), Chair (2012-2013), Past Chair (2014 – 2015) of SMU Grievance Commission

- Member of SMU China-India Strategy Task Force (2010)
- Member of SMU's Institutional Review Board (2006-2009)
- Member of SMU Provost Academic Committee (2006 – 2013)

Advisory Boards, Public and Professional Services

- Chair of Trust Tech Technical Committee (T2TC), Digital Trust Centre (DTC), IMDA, 1 October 2022 – 30 September 2027
- Core Member of the National Cybersecurity R&D Technical Review Panel (TRP), Cybersecurity Agency (CSA) Singapore, Jan 2022 - March 2026
- Member of the National Cybersecurity R&D (NCR) Programme Review - Sub-group 3 (2020)
- ACM Transactions on Privacy & Security EiC Search Committee (2020-2021)
- Evaluation Committee of the Trustworthy Software Systems National Satellite of Excellence (2019 – 2021)
- Scientific Advisory Board, Advanced Digital Sciences Center, Illinois at Singapore Pte Ltd (2019 – 2023)
- IEEE Reliability Society Fellow Committee (2019)
- Member of External Advisory Committee, Cybersecurity Research Centre, University of Technology Sydney (2018 – 2020)
- Member of Overseas Academic Advisory Committee, Cyber Security Research Institute, Zhejiang University (2018 - 2020)
- Member of International Consultant Committee, State Key Laboratory of Information Security (SKLOIS), Institute of Information Engineering, Chinese Academy of Science (2018 – 2020).
- External reviewer, Swiss National Science Foundation (SNSF) (2018)
- Member, ACM SIGSAC Awards Committee (2016 - 2017)
- Member, the IEEE CS Fellows Evaluation Committee (2016)
- Member, Advisory Board to European Union IST Sixth Framework project SMEPP (<http://www.smepp.org/>) (2007-2010)
- Member, Public Sector Funding Review Committee, Science and Engineering Research Council, Agency for Science, Technology and Research, Singapore (10/2007-09/2008)
- External Reviewer for the Research Grants Council (RGC) of Hong Kong (2007-2009)
- Board of Directors, ST Electronics (Info-Security) Pte Ltd (Company No: 199902746G) (2006-2011)
- Overseas referee for the evaluation of the 2006 State Natural Science Award of the People's Republic of China (2006)
- Judge, Tan Kah Kee Young Inventors Award, jointly organized by the Tan Kah Kee Foundations and the Agency for Science, Technology and Research, Singapore (2002, 2004, 2005)
- Technical Advisor, Trek 2000 International Ltd, Singapore (2003-2004)
- Member, National Science Scholarship Interview Panel, Agency for Science, Technology and Research, Singapore (2002-2004)
- Mentor for National Science Scholars Pursuing Science and Engineering Degrees (2002-2004)
- Member, Broadband Homes Working Group, Infocomm Development Agency, Singapore (2001-2003)
- Member, Review Panel for the Public Sector R&D Projects Funding Scheme, Agency for Science, Technology and Research, Singapore (2002)

- Member, Optical Network Focused Interest Group Steering Committee, Science and Engineering Research Council, Agency for Science, Technology and Research, Singapore (2002)
- Member, University Research Panel, National Science and Technology Board, Singapore (2001)
- Senior Visitor to the Institute of Mathematics Science Coding and Cryptography Program, National University of Singapore, Singapore (2001)
- Consultant, Data and Network Security, OCBC Bank, Singapore (2000-2001)
- Advisory Board, Internet Appliance Inc., Fremont, CA, USA (1999 – 2001)
- Consultant, Network for Electronic Transfers Singapore Pte Ltd (1996-1998)
- Associate and Management Committee Member of Magnetic Technology Center, National University of Singapore (1992-1996)
- Consultant, Wearnes Peripherals, Singapore (1993)
- Consultant, Seagate Technology, Singapore (1992)

Editorial Boards

- Editorial Board Member, *Information Security and Cryptography Book Series*, Springer (2020 - present)
- Guest Editor, *Special issue on Usable Security and Privacy for Large Model Systems*, *IET Information Security*, 2023-present
- Guest Editor, *Special issue on Data Fusion for Trust Evaluation*, *Information Fusion*, Vol. 76, December 2021.
- Associate Editor, *ACM Transactions on Privacy and Security (TOPS)* (01/2020-01/2022)
- Associate Editor, *3rd Edition of Encyclopedia of Cryptography, Security, and Privacy*, Springer (2019-present)
- Series Editor, SpringerBriefs in Information Security and Cryptography (2024-present)
- Series Editor, SpringerBriefs in Cyber Security Systems and Networks (2017-2023)
- Editorial Board, *IEEE Security and Privacy Magazine*, (01/2016-12/2020)
- Guest Editor, Special Issue on *5G-Enabled Intelligent Application for Distributed Industrial Internet-of-Things System*, *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 4, April 2022.
- Guest Editor, Special Issue on *Data Fusion for Trust Evaluation*, *Information Fusion*, August 2021.
- Guest Editor, *Special Issue on FinTech Security and Privacy*, *Future Generation Computer Systems*, Vol. 112, November 2020.
- Guest Editor, *Special Issue on Security and Privacy of Blockchain Technologies*, *International Journal of Information Security*, Vol. 19, No. 3, June 2020.
- Guest Editor, Special Issue on *Blockchain and Healthcare Computing*, *IEEE Journal of Biomedical and Health Informatics*, Vol. 24, No. 8, August 2020.
- Guest Editor, *Special Issue on Cryptography and Data Security in Cloud Computing*, *Information Sciences*, Elsevier, Vol. 387, May 2017.
- Guest Editor, *Special Issue on Trust Management for Multimedia Big Data*, *ACM Transactions on Multimedia Computing, Communications and Applications*, Vol. 12, No. 4s, November 2016.
- Guest Editor, *Special Issue on Security and Privacy of Electronic Health Information Systems*, *International Journal of Information Security*, Vol. 14, No. 6, November 2015.
- Guest Editor, *Special issue on Trust in Cyber, Physical and Social Computing*, *Computers & Security*, Vol. 47, November 2014.

- Guest Editor, *Special Issues on Trust in Cyber, Physical and Social Computing, Computer & Security*, Vol. 47, November, 2014
- Guest Editor, *Special Issue on Cryptography in Cloud Computing, Future Generation Computer Systems*, Vol. 30, January 2014.
- Editorial Board Member, *International Journal of Information Security*, Springer, (2013-2021)
- Editorial Board Member, *Special Issue on Security and Privacy in Complex Systems, IEEE Systems Journal*, Vol. 7, No. 3, September 2013.
- Member of Search Committee for the 2014-2015 Editor-in-Chief of *IEEE Transactions on Dependable and Secure Computing* (2012-2013)
- Associate Editor, *IEEE Transactions on Dependable and Secure Computing* (02/2012-02/2016)
- Guest Editor, *Special Issues on Trust and Identity Management in Mobile Internet, Computing and Communications, IET Information Security*, Vol. 7, No. 1, March 2013.
- Editorial Board, *International Journal of Multimedia Intelligence and Security*, Inderscience (2009 - 2017)
- Guest Editor, *Special Issue on Ubiquitous Electronic Commerce Systems, Journal of Electronic Commerce Research*, Vol. 11, No. 1, January 2011, Springer
- Associate Editor, *IEEE Transactions on Information Forensics and Security* (03/2009 – 03/2012)
- Associate Editor, *Security and Communication Networks Journal*, John Wiley and Sons (01/2007-12/2013)
- Editorial Board, *Journal of Computer Science and Technology (JCST)*, Institute of Computing Technology, Science Press, China and Springer Science + Business Media (2006 - 2018)
- Associate Editor, *International Journal of Internet Technology and Secured Transactions (IJITST)*, InderScience Publishers (2005 -2016)

Conference Committees

- **ACNS** - International Conference on Applied Cryptography and Network Security
 - PC Co-chair: 5-7 June 2019, Bogota, Colombia
 - PC Member: 16-19 October 2003, Kunming, China
 - PC Member, 6-9 June 2006, Singapore
 - PC Member, 22-25 June 2010, Beijing, China
 - PC Member, 7-10 June 2011, Nerja, Spain
 - PC Member, 26-29 June 2012, Singapore
- **ACSAC** - Annual Computer Security Applications Conference
 - PC Member, 8-12 December 2008, Anaheim, California, USA
 - PC Member, 7-11 December, 2009, Honolulu, Hawaii, USA
- **AsiaCCS** - ACM Asia Conference on Computer and Communications Security
 - Chair of Steering Committee (06/2013-05/2017)
 - Co-chair of Steering Committee (06/2012 – 05/2013)
 - Member of Steering Committee (06/2006 – 05/2012, 06/2017 - present)
 - PC Member, 21 – 24 March 2006, Taipei, Taiwan
 - PC Co-chair, 20-22 March 2007, Singapore
 - PC Member, 18 -20 March 2008, Tokyo, Japan
 - PC Member, 10-12 March 2009, Sydney, Australia
 - PC Member, 13-16 April 2010, Beijing, China
 - PC Member, 22-24 March 2011, Hong Kong, China
 - PC Member, 1-3 May 2012, Seoul, Korea
 - PC Member, 8-10 May 2013, Hangzhou, China

- **AsiaCrypt**
 - PC Member, 30 November – 4 December 2003, Taipei, Taiwan
- **CANS** - International Conference on Cryptology and Network Security
 - PC Co-chair, 25-27 October 2019, Fuzhou, China
 - PC Member, 8-10 December 2007, Singapore
 - PC Member, 2-4 December 2008, Hong Kong
- **CCS** - ACM Conference on Computer and Communications Security
 - PC Member, 1-4 November 1999, Singapore
 - PC Member, 29 October – 2 November 2007, Alexandria, Virginia, USA
 - PC Member, 27-31 October 2008, Alexandria, Virginia, USA
 - PC Member, 16-18 October 2012, Raleigh, NC, USA
- **CSS** - International Symposium on Cyberspace Safety and Security
 - PC Member, 13-14 November 2013, Zhangjiajie, China
 - PC co-chair, 20-22 August 2014, Paris, France
- **DSC** - IEEE Conference on Dependable and Secure Computing
 - PC co-chair, 30 Jan – 2 Feb 2021, Aizuwakamatsu, Japan
 - Steering Committee Member (2017-2022)
- **DSI** - National Decision Sciences Institute Annual Meeting,
 - Co-Chair, Information Security Track, 17-20 November 2007, Phoenix, Arizona, USA
- **ESORICS** - European Symposium on Research in Computer Security
 - PC Member, 18-20 September 2006, Hamburg, Germany
 - PC Member, 24-26 September 2007, Dresden, Germany
- **ICICS** - International Conference on Information and Communications Security
 - Steering Committee 2019 - present
 - PC Member, 11-14 November 1997, Beijing, China
 - PC Member, 9-11 November 1999, Sydney, Australia
 - PC Co-Chair, 9-12 December 2002, Singapore
 - PC Member, 10-13 October 2003, Huhehote, China
 - PC Member, 27-29 October 2004, Malaga, Spain
 - PC Member, 10-13 December 2005, Beijing, China
 - PC Member, 12-15 December 2007, Zhengzhou, China
 - PC Member, 20-22 October 2008, Birmingham, UK
- **IEEE Blockchain** - IEEE International Conference on Blockchain
- **General co-chair**, 6-8 December 2021, Melbourne, Australia
- **Inscrypt** - International Conference on Information Security and Cryptology
 - PC Member, 31 August – 5 September 2007, Xining, Qinghai, China
 - PC Member, 12-15 December 2009, Beijing, China
 - PC Member, 20-23 October 2010, Shanghai, China
- **Intrust** - International Conference on Trusted Systems
 - Member of Steering Committee (2009-2020)
 - General Co-Chair, 17th – 19th December 2009, Beijing, China
 - General Co-Chair, 13 – 15 December 2010, Beijing, China
 - General Co-Chair, 27-29 November 2011, Beijing, China
- **ISC** - Information Security Conference
 - PC chair, 16 – 20 December 2020, Bali, Indonesia
 - General Co-chair, 20-23 September 2005, Singapore
 - PC Member, 15-18 September 2008, Taipei, Taiwan

- PC Member, 9-11 September 2015, Trondheim, Norway
- **ISPEC** - Information Security Practice and Experience Conference
 - Member of Steering Committee (2005-present)
 - General Chair, 11-14 April, 2005, Singapore
 - PC Co-chair, 11 – 14 April 2006, Hangzhou, China
 - PC Member, 7-10 May, Hong Kong, China
 - General Co-chair, 13-15 April 2009, Xi'an, China
 - PC Co-chair, 12-13 May 2010, Seoul, Korea
 - PC Co-chair, 16-18 November, Zhangjiajie, China
 - General Co-chair, 14-16 May 2011, Guangzhou, China
 - General Co-Chair, 9-12 April 2012, Hangzhou, China
 - PC Co-chair, 12-14 May 2013, Lanzhou, China
 - General Co-chair, 12-14 May 2014, Fuzhou, China
 - General Co-chair, 5-8 May, 2015, Beijing, China
 - PC Co-chair, 16-18 November 2016, Zhangjiajie, China
 - General Co-chair, 13-15 December 2017, Melbourne, Australia
 - Honorary Chair, 23-25 December 2022, Taipei, Taiwan
 - General Chair, 24-25 August 2023, DTU Modecenter, Denmark
- **MINES** – International Conference on Multimedia Information Networking and Security
 - TPC Co-chair, 18-20 November 2009, Wuhan, China
 - TPC Co-chair, 4-6 November 2010, Nanjing, China
 - TPC Co-chair, 4-6 November 2011, Shanghai, China
 - TPC Co-chair, 2-4 November 2012, Nanjing, China
- **NSS** - International Conference on Network and System Security
 - Steering committee member (2012 – present)
 - PC Member, 20 September 2007, Dalian, China
 - PC Member, 18-19 September 2008, Shanghai, China
 - PC Member, 19-20 October 2009, Gold Coast, Australia
 - PC Member, 21-23 November 2012, Fujian, China
- **PKC** - International Public Key Cryptosystems Workshop
 - General Chair and PC Member, 1-4 March 2004, Singapore
- **SACMAT** - ACM Symposium on Access Control Models and Technologies
 - Steering Committee Member, July 2017 – June 2023
- **SecureComm** - International Conference on Security and Privacy in Communication Networks
 - General Chair, 28-30 October 2024, Dubai, UAE
 - General Co-Chair, 10-12 September 2016, Guangzhou, China
 - TPC Member, 5-9 September 2005, Athens, Greece
 - TPC Member, 28 August – 1 September 2006, Baltimore, USA
- **S&P** - IEEE Symposium on Security and Privacy
 - PC Member, 9-12 May 1999, Oakland, California, USA
 - PC Member, 14-17 May 2000, Oakland, California, USA
- **SpaCCS**- International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage
 - Steering Committee Member (11/2015-present)
 - General Co-Chair, December 12-15, 2017, Guangzhou, China
- **WiSec** – ACM Conference on Wireless Network Security
 - PC Member, 14-17 June 2011, Hamburg, Germany

6 Publications

Books and Chapters in Books

1. Robert Deng, Feng Bao, Guilin Wang, Jian Shen, Mark Ryan, Weizhi Meng, Ding Wang (Eds), *Information Security and Practice*, Lecture Notes in Computer Science, LNCS 13107, 394 pages, Springer, 2021.
2. Willy Susilo, Robert H. Deng, Fuchun Guo, Yannan Li, Rolly Intan (Eds), *Information Security*, Lecture Notes on Computer Science, LNCS 12472, 426 pages, Springer, 2020.
3. Yi Mu, Robert H. Deng, and Xinyi Huang (Eds), *Cryptology and Network Security*, Lecture Notes on Computer Science, LNCS 11829, 540 pages, Springer, 2019
4. Robert H. Deng, Valerie Gauthier-Umana, Martin Ochoa, and Moti Yung (Eds), *Applied Cryptography and Network Security*, Lecture Notes on Computer Science, LNCS 11464, 614 pages, Springer, 2019.
5. David Lee and Robert Deng (Eds), *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1 - Cryptocurrency, FinTech, InsurTech, and Regulation*, 482 pages, ISBN: 9780128104415, Elsevier, August 2017.
6. David Lee and Robert Deng (Eds), *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2 - ChinaTech, Mobile Security, and Distributed Ledger*, 554 pages, ISBN: 9780128122822, Elsevier, August 2017.
7. Robert Deng, Jian Weng, Kui Ren, and Vinod Yegneswaran (Eds), *Security and Privacy in Communication Networks*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 198, 781 pages, Springer, 2017.
8. Feng Bao, Liqun Chen, Robert H. Deng and Guojun Wang (Eds), *Information Security Practice and Experience*, Lecture Notes in Computer Science 10060, 377 pages, Springer 2016.
9. Yingjiu Li, Qiang Yan, and Robert H. Deng, *Leakage Resilient Password Systems*, 74 pages, Springer, January 2015.
10. Robert H. Deng, Elaine Shi and Kui Ren (Eds), *Proceedings of the Second International Workshop on Security in Cloud Computing*, SCC@ASIACCS2014, Kyoto, Japan, June 3, 2014. ACM 2014, 68 pages, ISBN 978-1-4503-2805-0.
11. Yingjiu Li, Robert H. Deng and Elisa Bertino, *RFID Security and Privacy*, Synthesis Lectures on Information Security, Privacy, and Trust, Morgan & Claypool Publishers, 157 pages, December 2013.
12. Qiang Yan, Yingjiu Li, and Robert H. Deng, “Malware protection on RFID-enabled supply chain management systems in the EPCglobal network”, Ali Miri (Ed), *Advanced Security and Privacy for RFID Technologies*, pp. 153-175, IGI Global 2013.
13. Robert H. Deng and Tao Feng (Eds), *Information Security Practice and Experience*, Lecture Notes in Computer Science 7863, 386 pages, Springer 2013.
14. Sherman S. M. Chow, Cheng-Kang Chu, Xinyi Huang, Jianying Zhou and Robert H. Deng, “Dynamic secure cloud storage with provenance”, David Naccache (Ed), *Cryptography and Security: From Theory to Applications*, pp. 442-464, Springer LNCS 6805, 2012.
15. Jin Kwak, Robert H. Deng, Yoojae Won, and Ghilin Wang (Eds), *Information Security Practice and Experience*, Lecture Notes in Computer Science 6047, 399 pages, Springer 2010.
16. Xuhua Ding, Liang Gu, Robert H. Deng, Bing Xie, Hong Mei, “Remote platform attestation – the testimony for trust management”, Zheng Yan (Eds), *Trust Modelling and Management*

in Digital Environments: From Social Concept to System Development, pp. 1-19, IGI Global, 2010.

17. Robert H. Deng and Pierangela Samarati (Eds), *Proceedings of the ACM Symposium on Information, Computer and Communications Security*, 401 pages, ACM Press 2007.
18. Kefei Chen, Robert H. Deng, Xuejia Lai and Jianying Zhou (Eds), *Information Security Practice and Experience*, Lecture Notes in Computer Science 3906, 389 pages, Springer 2006.
19. Jianying Zhou, Javier Lopez, Robert H. Deng and Feng Bao, (Eds), *Information Security*, Lecture Notes in Computer Science 3650, 516 pages, Springer 2005.
20. Robert. H. Deng, Feng Bao, HweeHwa Pang and Jianying Zhou (Eds), *Information Security Practice and Experience*, Lecture Notes in Computer Science 3439, 417 pages, Springer 2005.
21. Robert H. Deng, Yongdong Wu and Di Ma, "Securing JPEG2000 code-streams", D. T. Lee, S. Shieh and D. J. Tygar (Eds.), pp. 229-253, *Computer Security in the 21st Century*, 268 pages, Springer 2005.
22. Feng Bao, Robert H. Deng and Jianying Zhou (Eds.), *Public Key Cryptography*, 454 pages, *Lecture Notes in Computer Science 2947*, Springer 2004.
23. Robert H. Deng, Sihang Qing, Feng Bao and Jianying Zhou (Eds.), *Information and Communications Security*, 496 pages, *Lecture Notes in Computer Science 2513*, Springer, 2002
24. Mark A. Herro, Robert H. Deng, and Yuanxin Li, "Charge constrained convolutional codes," R. E. Blahu, D. J. Costello, Jr., U. Maurer, and T. Mittelholzer (Eds.), *Communications and Cryptography: Two Sides of One Trapestry*, Kluwer Academic Publishers, Boston, pp. 173-177, 1994.

Referred Journal Publications

1. Feng Li, Jianfeng Ma, Yinbin Miao, Ximeng Liu, Jianting Ning, Robert H. Deng, "A survey on searchable symmetric encryption", *ACM Computing Survey*, 56(5), pp. 119:1 – 119:42, May 2024.
2. Yunbo Yang, Yiwei Hu, Xiaolei Dong, Jiachen Shen, Zhenfu Cao, Guomin Yang, Robert H. Deng, "OpenSE: efficient verifiable searchable encryption with access and search pattern hidden for cloud-IoT", *IEEE Internet Things Journal*, 11(8), pp. 13793-13809, April 2024.
3. Shuqin Liu, Yinbin Miao, Feng Li, Xinghua Li, Kim-Kwang Raymond Choo, Robert H. Deng, "Practical revocable keyword search over mobile cloud-assisted Internet of Things", *IEEE Internet Things J.* 11(16), pp. 27494-27508, August 2024.
4. Yiwei Zhang, Siqi Ma, Tiancheng Chen, Juanru Li, Robert H. Deng, Elisa Bertino, "EvilScreen attack: smart TV hijacking via multi-channel remote control mimicry", *IEEE Trans. Dependable Secur. Comput.* 21(4), pp. 1544-1556, July-August 2024.
5. Yang Yang, Wenyi Xue, Yonghua Zhan, Minming Huang, Yingjiu Li, Robert H. Deng, "AnoPay: anonymous payment for vehicle parking with updatable credential", *IEEE Trans. Dependable Secur. Comput.* 21(4), pp. 1621-1638, July-August 2024.
6. Guowen Xu, Xingshuo Han, Tianwei Zhang, Shengmin Xu, Jianting Ning, Xinyi Huang, Hongwei Li, Robert H. Deng, "SIMC 2.0: improved secure ML inference against malicious clients", *IEEE Trans. Dependable Secur. Comput.* 21(4), pp. 1708-1723, July-August 2024.
7. Yinbin Miao, Feng Li, Xinghua Li, Jianting Ning, Hongwei Li, Kim-Kwang Raymond Choo, Robert H. Deng, "Verifiable outsourced attribute-based encryption scheme for cloud-assisted mobile e-health system", *IEEE Trans. Dependable Secur. Comput.* 21(4), pp. 1845-1862, July-

August 2024.

8. Yinbin Miao, Ziteng Liu, Xinghua Li, Meng Li, Hongwei Li, Kim-Kwang Raymond Choo, Robert H. Deng, “Robust asynchronous federated learning with time-weighted and stale model aggregation”, *IEEE Trans. Dependable Secur. Comput.* 21(4), pp. 2361-2375, July-August 2024.
9. Rui Shi, Yang Yang, Yingjiu Li, Huamin Feng, Guozhen Shi, HweeHwa Pang, Robert H. Deng, “Double issuer-hiding attribute-based credentials from tag-based aggregatable mercurial signatures”, *IEEE Trans. Dependable Secur. Comput.* 21(4), pp. 2585-2602, July-August 2024.
10. Man Zhang, Xinghua Li, Yanbing Ren, Bin Luo, Yinbin Miao, Ximeng Liu, Robert H. Deng, “Privacy-preserved data trading via verifiable data disturbance”, *IEEE Trans. Dependable Secur. Comput.* 21(4), pp. 3126-3140, July – August 2024.
11. Yinbin Miao, Feng Li, Xiaohua Jia, Huaxiong Wang, Ximeng Liu, Kim-Kwang Raymond Choo, Robert H. Deng, “REKS: role-based encrypted keyword search with enhanced access control for outsourced cloud data”, *IEEE Trans. Dependable Secur. Comput.* 21(4), pp. 3247-3261, July – August 2024.
12. Yinbin Miao, Rongpeng Xie, Xinghua Li, Zhiquan Liu, Kim-Kwang Raymond Choo, Robert H. Deng, “Efficient and secure federated learning against backdoor attacks”, *IEEE Trans. Dependable Secur. Comput.* 21(5): 4619-4636, Sept-Oct, 2024.
13. Ju Jia, Siqi Ma, Yang Liu, Lina Wang, Robert H. Deng, “A causality-aligned structure rationalization scheme against adversarial biased perturbations for graph neural networks”, *IEEE Trans. Inf. Forensics Secur.* 19, pp. 59-73, 2024.
14. Zekai Chen, Shengxing Yu, Mingyuan Fan, Ximeng Liu, Robert H. Deng, “Privacy-enhancing and robust backdoor defense for federated learning on heterogeneous data”, *IEEE Trans. Inf. Forensics Secur.* 19, pp. 693-707, 2024.
15. Xiaoguo Li, Zixi Huang, Bowen Zhao, Guomin Yang, Tao Xiang, Robert H. Deng, “STDA: secure time series data analytics with practical efficiency in wide-area network”, *IEEE Trans. Inf. Forensics Secur.* 19, pp. 1440-1454, 2024.
16. Jianchang Lai, Willy Susilo, Robert H. Deng, Fuchun Guo, “SDSS: sequential data sharing system in IoT”, *IEEE Trans. Inf. Forensics Secur.* 19, pp. 2288-2299, 2024.
17. Qiuyun Tong, Xinghua Li, Yinbin Miao, Yunwei Wang, Ximeng Liu, Robert H. Deng, “Beyond result verification: efficient privacy-preserving spatial keyword query with suppressed leakage”, *IEEE Trans. Inf. Forensics Secur.* 19, pp. 2746-2760, 2024.
18. Man Zhang, Xinghua Li, Yinbin Miao, Bin Luo, Wanyun Xu, Yanbing Ren, Robert H. Deng, “Privacy-preserved data disturbance and truthfulness verification for data trading”, *IEEE Trans. Inf. Forensics Secur.* 19, pp. 5545-5560, 2024.
19. Bowen Zhao, Weiquan Deng, Xiaoguo Li, Ximeng Liu, Qingqi Pei, Robert H. Deng, “SOCI+: An enhanced toolkit for secure outsourced computation on integers”, *IEEE Trans. Inf. Forensics Secur.* 19, pp. 5607-5619, 2024.
20. Yinbin Miao, Xinru Yan, Xinghua Li, Shujiang Xu, Ximeng Liu, Hongwei Li, Robert H. Deng, “RFed: robustness-enhanced privacy-preserving federated learning against poisoning attack”, *IEEE Trans. Inf. Forensics Secur.* 19, pp. 5814-5827, 2024.
21. Yinbin Miao, Da Kuang, Xinghua Li, Shujiang Xu, Hongwei Li, Kim-Kwang Raymond Choo, Robert H. Deng, “Privacy-preserving asynchronous federated learning under non-IID settings,

IEEE Trans. Inf. Forensics Secur. 19, pp. 5828-5841, 2024.

22. Yang Yang, Wenyi Xue, Jianfei Sun, Guomin Yang, Yingjiu Li, HweeHwa Pang, Robert H. Deng, "PkT-SIN: a secure communication protocol for space information networks with periodic k-time anonymous authentication", *IEEE Trans. Inf. Forensics Secur.* 19, pp. 6097-6112, 2024.
23. Mengdi Hu, Lanxiang Chen, Gaolin Chen, Yi Mu, Robert H. Deng, "A pruned pendant vertex based index for shortest distance query under structured encrypted graph", *IEEE Trans. Inf. Forensics Secur.* 19, pp. 6351-6363, 2024.
24. Zekai Chen, Shengxing Yu, Farong Chen, Fuyi Wang, Ximeng Liu, Robert H. Deng, "Lightweight privacy-preserving cross-cluster federated learning with heterogeneous data", *IEEE Trans. Inf. Forensics Secur.* 19, pp. 7404-7419, 2024.
25. Zhe Chen, Haiyan Zhang, Xinghua Li, Yinbin Miao, Xiaohan Zhang, Man Zhang, Siqi Ma, Robert H. Deng, "FDFL: Fair and discrepancy-aware incentive mechanism for federated learning", *IEEE Trans. Inf. Forensics Secur.* 19, pp. 8140-8154, 2024.
26. Yanrong Liang, Jianfeng Ma, Yinbin Miao, Yuan Su, Robert H. Deng, "Efficient and privacy-preserving encode-based range query over encrypted cloud data", *IEEE Trans. Inf. Forensics Secur.* 19, pp. 9085-9099, 2024.
27. Yinbin Miao, Yutao Yang, Xinghua Li, Linfeng Wei, Zhiquan Liu, Robert H. Deng, "Efficient privacy-preserving spatial data query in cloud computing", *IEEE Trans. Knowl. Data Eng.* 36(1), 122-136, 2024.
28. Zhuoran Ma, Yang Liu, Yinbin Miao, Guowen Xu, Ximeng Liu, Jianfeng Ma, Robert H. Deng, "FIgan: GAN-based unbiased federated learning under non-IID settings", *IEEE Trans. Knowl. Data Eng.* 36(4), pp. 1566-1581, 2024.
29. Haiyan Zhang, Xinghua Li, Mengfan Xu, Ximeng Liu, Tong Wu, Jian Weng, Robert H. Deng, "BADFL: Backdoor attack defense in federated learning from local model perspective", *IEEE Trans. Knowl. Data Eng.* 36(11), pp.5661-5674, 2024.
30. Yinbin Miao, Feng Li, Xinghua Li, Zhiquan Liu, Jianting Ning, Hongwei Li, Kim-Kwang Raymond Choo, Robert H. Deng, "Time-controllable keyword search scheme with efficient revocation in mobile e-health cloud", *IEEE Trans. Mob. Comput.* 23(5), pp. 3650-3665, 2024.
31. Zhe Ren, Xinghua Li, Yinbin Miao, Zhuowen Li, Zihao Wang, Mengyao Zhu, Ximeng Liu, Robert H. Deng, "Intelligent adaptive gossip-based broadcast protocol for UAV-MEC using multi-agent deep reinforcement learning", *IEEE Trans. Mob. Comput.* 23(6), pp. 6563-6578, 2024.
32. Yinbin Miao, Lin Song, Xinghua Li, Hongwei Li, Kim-Kwang Raymond Choo, Robert H. Deng, "Privacy-preserving arbitrary geometric range query in mobile Internet of vehicles", *IEEE Trans. Mob. Comput.* 23(7), pp. 7725-7738, 2024.
33. Zihao Wang, Hang Wang, Zhuowen Li, Xinghua Li, Yinbin Miao, Yanbing Ren, Yunwei Wang, Zhe Ren, Robert H. Deng, "Robust permissioned blockchain consensus for unstable communication in FANET", *IEEE/ACM Trans. Netw.* 32(1), pp. 699-712, 2024.
34. Bin Luo, Xinghua Li, Yinbin Miao, Man Zhang, Ximeng Liu, Yanbing Ren, Xizhao Luo, Robert H. Deng, "PAM3S: progressive two-stage auction-based multi-platform multi-user mutual selection scheme in MCS", *IEEE/ACM Trans. Netw.* 32(1), pp. 729-744, 2024.
35. Xinru Yan, Yinbin Miao, Xinghua Li, Kim-Kwang Raymond Choo, Xiangdong Meng, Robert H. Deng, "Privacy-Preserving Asynchronous Federated Learning Framework in Distributed

- IoT”, *IEEE Internet Things J.* 10(15): 13281-13291, 2023.
36. Peilei Xue, Xinghua Li, Zhongyuan Jiang, Bin Luo, Yinbin Miao, Ximeng Liu, Robert H. Deng, “A Multi-CUAV Multi-UAV Electricity Scheduling Scheme: From Charging Location Selection to Electricity Transaction”, *IEEE Internet Things J.* 10(23): 20899-20913, 2023.
 37. Yuxian Li, Jian Weng, Wei Wu, Ming Li, Yingjiu Li, Haoxin Tu, Yongdong Wu, Robert H. Deng, “PRI: PCH-based privacy-preserving with reusability and interoperability for enhancing blockchain scalability”, *J. Parallel Distributed Comput.* 180: 104721, 2023.
 38. Yanrong Liang, Jianfeng Ma, Yinbin Miao, Da Kuang, Xiangdong Meng, Robert H. Deng, “Privacy-Preserving Bloom Filter-Based Keyword Search Over Large Encrypted Cloud Data”, *IEEE Trans. Computers* 72(11): 3086-3098, 2023.
 39. Yang Yang, Robert H. Deng, Wenzhong Guo, Hongju Cheng, Xiangyang Luo, Xianghan Zheng, Chunming Rong, “Dual Traceable Distributed Attribute-Based Searchable Encryption and Ownership Transfer”, *IEEE Trans. Cloud Comput.* 11(1): 247-262, 2023.
 40. Jianfei Sun, Guowen Xu, Tianwei Zhang, Hu Xiong, Hongwei Li, Robert H. Deng, “Share Your Data Carefree: An Efficient, Scalable and Privacy-Preserving Data Sharing Service in Cloud Computing”, *IEEE Trans. Cloud Comput.* 11(1): 822-838, 2023.
 41. Feng Li, Jianfeng Ma, Yinbin Miao, Zhiquan Liu, Kim-Kwang Raymond Choo, Ximeng Liu, Robert H. Deng, “Towards Efficient Verifiable Boolean Search Over Encrypted Cloud Data”, *IEEE Trans. Cloud Comput.* 11(1): 839-853, 2023.
 42. Shengmin Xu, Jianting Ning, Yingjiu Li, Yinghui Zhang, Guowen Xu, Xinyi Huang, Robert H. Deng, “A Secure EMR Sharing System With Tamper Resistance and Expressive Access Control”, *IEEE Trans. Dependable Secur. Comput.* 20(1): 53-67, 2023.
 43. Rui Zhang, Zheng Yan, Xuerui Wang, Robert H. Deng, “VOLERE: Leakage Resilient User Authentication Based on Personal Voice Challenges”, *IEEE Trans. Dependable Secur. Comput.* 20(2): 1002-1016, 2023.
 44. Hua Deng, Zheng Qin, Qianhong Wu, Robert H. Deng, Zhenyu Guan, Yupeng Hu, Fangmin Li, “Achieving Fine-Grained Data Sharing for Hierarchical Organizations in Clouds,” *IEEE Trans. Dependable Secur. Comput.* 20(2): 1364-1377, 2023.
 45. Boyu Kuang, Anmin Fu, Yansong Gao, Yuqing Zhang, Jianying Zhou, Robert H. Deng, “FeSA: Automatic Federated Swarm Attestation on Dynamic Large-Scale IoT Devices”, *IEEE Trans. Dependable Secur. Comput.* 20(4): 2954-2969, 2023.
 46. Xiangyu Wang, Jianfeng Ma, Ximeng Liu, Yinbin Miao, Yang Liu, Robert H. Deng, “Forward/Backward and Content Private DSSE for Spatial Keyword Queries”, *IEEE Trans. Dependable Secur. Comput.* 20(4): 3358-3370, 2023.
 47. Lei Zhou, Anmin Fu, Guomin Yang, Yansong Gao, Shui Yu, Robert H. Deng, “Fair Cloud Auditing Based on Blockchain for Resource-Constrained IoT Devices”, *IEEE Trans. Dependable Secur. Comput.* 20(5): 4325-4342, 2023.
 48. Guowen Xu, Xingshuo Han, Shengmin Xu, Tianwei Zhang, Hongwei Li, Xinyi Huang, Robert H. Deng, “Hercules: Boosting the Performance of Privacy-Preserving Federated Learning”, *IEEE Trans. Dependable Secur. Comput.* 20(5): 4418-4433, 2023.
 49. Zhuoran Ma, Jianfeng Ma, Yinbin Miao, Ximeng Liu, Wei Zheng, Kim-Kwang Raymond Choo, Robert H. Deng, “VerifyTL: Secure and Verifiable Collaborative Transfer Learning”, *IEEE Trans. Dependable Secur. Comput.* 20(6): 5087-5101, 2023.
 50. Shengmin Xu, Xinyi Huang, Jiaming Yuan, Yingjiu Li, Robert H. Deng, “Accountable and

- Fine-Grained Controllable Rewriting in Blockchains”, *IEEE Trans. Inf. Forensics Secur.* 18: 101-116, 2023.
51. Jianfei Sun, Guowen Xu, Tianwei Zhang, Xuehuan Yang, Mamoun Alazab, Robert H. Deng, “Verifiable, Fair and Privacy-Preserving Broadcast Authorization for Flexible Data Sharing in Clouds”, *IEEE Trans. Inf. Forensics Secur.* 18: 683-698, 2023.
 52. Lanxiang Chen, Yi Mu, Lingfang Zeng, Fatemeh Rezaeibagha, Robert H. Deng, “Authenticable Data Analytics Over Encrypted Data in the Cloud”, *IEEE Trans. Inf. Forensics Secur.* 18: 1800-1813, 2023.
 53. Yinbin Miao, Wei Zheng, Xinghua Li, Hongwei Li, Kim-Kwang Raymond Choo, Robert H. Deng, “Secure Model-Contrastive Federated Learning with Improved Compressive Sensing”, *IEEE Trans. Inf. Forensics Secur.* 18: 3430-3444, 2023.
 54. Wenyi Xue, Yang Yang, Yingjiu Li, HweeHwa Pang, Robert H. Deng, “ACB-Vote: Efficient, Flexible, and Privacy- Preserving Blockchain-Based Score Voting with Anonymously Convertible Ballots”, *IEEE Trans. Inf. Forensics Secur.* 18: 3720-3734, 2023.
 55. Yinbin Miao, Yutao Yang, Xinghua Li, Zhiquan Liu, Hongwei Li, Kim-Kwang Raymond Choo, Robert H. Deng, “Efficient Privacy-Preserving Spatial Range Query Over Outsourced Encrypted Data”, *IEEE Trans. Inf. Forensics Secur.* 18: 3921-3933, 2023.
 56. Jianfei Sun, Guowen Xu, Tianwei Zhang, Xuehuan Yang, Mamoun Alazab, Robert H. Deng, “Privacy-Aware and Security-Enhanced Efficient Matchmaking Encryption”, *IEEE Trans. Inf. Forensics Secur.* 18: 4345-4360, 2023.
 57. Xueqiao Liu, Guomin Yang, Willy Susilo, Kai He, Robert H. Deng, Jian Weng, “Privacy-Preserving Multi-User Outsourced Computation for Boolean Circuits”, *IEEE Trans. Inf. Forensics Secur.* 18: 4929-4943, 2023.
 58. Bowen Zhao, Xiaoguo Li, Ximeng Liu, Qingqi Pei, Yingjiu Li, Robert H. Deng, “CrowdFA: A Privacy-Preserving Mobile Crowdsensing Paradigm via Federated Analytics”, *IEEE Trans. Inf. Forensics Secur.* 18: 5416-5430, 2023.
 59. Rui Zhang, Zheng Yan, Xuerui Wang, Robert H. Deng, “LiVoAuth: Liveness Detection in Voiceprint Authentication With Random Challenges and Detection Modes”, *IEEE Trans. Inf. Forensics Secur.* 19(6): 7676-7688, 2023.
 60. Qiuyun Tong, Xinghua Li, Yinbin Miao, Ximeng Liu, Jian Weng, Robert H. Deng, “Privacy-Preserving Boolean Range Query With Temporal Access Control in Mobile Computing”, *IEEE Trans. Knowl. Data Eng.* 35(5): 5159-5172, 2023.
 61. Qiuyun Tong, Yinbin Miao, Jian Weng, Ximeng Liu, Kim-Kwang Raymond Choo, Robert H. Deng, “Verifiable Fuzzy Multi-Keyword Search Over Encrypted Data with Adaptive Security”, *IEEE Trans. Knowl. Data Eng.* 35(5): 5386-5399, 2023.
 62. Yanbing Ren, Xinghua Li, Yinbin Miao, Robert H. Deng, Jian Weng, Siqi Ma, Jianfeng Ma, “DistPreserv: Maintaining User Distribution for Privacy-Preserving Location-Based Services”, *IEEE Trans. Mob. Comput.* 22(6): 3287-3302, 2023.
 63. Qiuyun Tong, Yinbin Miao, Hongwei Li, Ximeng Liu, Robert H. Deng, “Privacy-Preserving Ranked Spatial Keyword Query in Mobile Cloud-Assisted Fog Computing”, *IEEE Trans. Mob. Comput.* 22(6): 3604-3618, 2023.
 64. Bowen Zhao, Ximeng Liu, Wei-Neng Chen, Robert H. Deng, “CrowdFL: Privacy-Preserving Mobile Crowdsensing System Via Federated Learning”, *IEEE Trans. Mob. Comput.* 22(8): 4607-4619, 2023.

65. Qiuyun Tong, Xinghua Li, Yinbin Miao, Yunwei Wang, Ximeng Liu, Robert H. Deng, “Owner-free Distributed Symmetric Searchable Encryption Supporting Conjunctive Queries”, *ACM Trans. Storage* 19(4): 38:1-38:25, 2023.
66. Yinbin Miao, Wei Zheng, Xiaohua Jia, Ximeng Liu, Kim-Kwang Raymond Choo, Robert H. Deng, “Ranked Keyword Search Over Encrypted Cloud Data Through Machine Learning Method”, *IEEE Trans. Serv. Comput.* 16(1): 525-536, 2023.
67. Lanxiang Chen, Yujie Xue, Yi Mu, Lingfang Zeng, Fatemeh Rezaeibagha, Robert H. Deng, “CASE-SSE: Context-Aware Semantically Extensible Searchable Symmetric Encryption for Encrypted Cloud Data”, *IEEE Trans. Serv. Comput.* 16(2): 1011-1022, 2023.
68. Rui Shi, Huamin Feng, Yang Yang, Feng Yuan, Yingjiu Li, HweeHwa Pang, Robert H. Deng, “Threshold Attribute-Based Credentials With Redactable Signature”, *IEEE Trans. Serv. Comput.* 16(5): 3751-3765, 2023.
69. Zhan Zhang, Xinghua Li, Yunwei Wang, Yinbin Miao, Ximeng Liu, Jian Weng, Robert H. Deng, “TAGKA: Threshold Authenticated Group Key Agreement Protocol Against Member Disconnect for UANET”, *IEEE Trans. Veh. Technol.* 72(11): 14987-15001, 2023.
70. Bowen Zhao, Jiaming Yuan, Ximeng Liu, Yongdong Wu, Hwee Hwa Pang, Robert H. Deng, “SOCl: A Toolkit for Secure Outsourced Computation on Integers”, *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp. 3637-3648, 2022.
71. Jianfei Sun, Guowen Xu, Tianwei Zhang, Mamoun Alazab, Robert H. Deng, “A practical fog-based privacy-preserving online car-hailing service system”, *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp. 2862-2877, 2022.
72. Yinbin Miao, Ziteng Liu, Hongwei Li, Kim-Kwang Raymond Choo, Robert H. Deng, “Privacy-preserving Byzantine-robust federated learning via blockchain systems”, *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp. 2848-2861, 2022.
73. Zhenzhu Chen, Shang Wang, Anmin Fu, Yansong Gao, Shui Yu, Robert H. Deng, “LinkBreaker: breaking the backdoor-trigger link in DNNs via neurons consistency check”, *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp. 2000-2014, 2022.
74. Zhuoran Ma, Jianfeng Ma, Yinbin Miao, Yingjiu Li, Robert H. Deng, “ShieldFL: mitigating model poisoning attacks in privacy-preserving federated learning”, *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp. 1639-1654, 2022.
75. Jinhua Ma, Shengmin Xu, Jianting Ning, Xinyi Huang, Robert H. Deng, “Redactable blockchain in decentralized setting”, *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp. 1227-1242, 2022.
76. Yanbing Ren, Xinghua Li, Yinbin Miao, Bin Luo, Jian Weng, Kim-Kwang Raymond Choo, Robert H. Deng, “Towards privacy-preserving spatial distribution crowdsensing: a gamet theoretic approach”, *IEEE Transactions on Information Forensics and Security*, Vol. 17, pp. 804-818, 2022.
77. Huiying Hou, Jianting Ning, Yunlei Zhao, Robert H. Deng, “Fine-grained and controllably editable data sharing with accountability in cloud storage”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 5, pp. 3448-3463, Sept-Oct 2022.
78. Huiying Hou, Jianting Ning, Yunlei Zhao, Robert H. Deng, “A traitor-resistant and dynamic anonymous communication service for cloud-based VANETs”, *IEEE Trans. Serv. Comput.* Vol. 15, No. 5, pp. 2551-2564, Sept-Oct 2022.
79. Lin Song, Yinbin Mao, Jian Weng, Kim-Kwang Raymond Choo, Ximeng Liu, Robert H.

- Deng, “Privacy-preserving threshold-based image retrieval in cloud-assisted Internet of Things”, *IEEE Internet of Things Journal*, Vol. 9, Np. 15, pp. 13598-13611, August 2022.
80. Yujie Xue, Lanxiang Chen, Yi Mu, Lingfang Zeng, Fatemeh Rezaeibagha, Robert H. Deng, “Structured encryption for knowledge graphs”, *Information Sciences*, Vol. 605, pp. 43-70, August 2022.
 81. Zheng Yan, Xinren Qian, Shushu Liu, Robert H. Deng, “Privacy Protection in 5G Positioning and Location-based Services Based on SGX”, *ACM Trans. Sens. Networks*, Vo. 18, No. 3, pp. 41:1-41:19, August 2022.
 82. Yang Yang, Robert H. Deng, Ximeng Liu, Yongdong Wu, Jian Weng, Xianghan Zheng, Chunming Rong, “Privacy-preserving medical treatment system through nondeterministic finite automata”, *IEEE Trans. Cloud Comput.* Vol. 10, No. 3, pp. 2020-2037, July – Sept 2022.
 83. Yilin Li, Shushu Liu, Zheng Yan, Robert H. Deng, “Secure 5G positioning with truth discovery, attack detection, and tracing”, *IEEE Internet Things Journal*, Vol 19, No. 22, pp. 22220-22229, Nov 2022.
 84. Tong Liu , Yinbin Miao , Kim-Kwang Raymond Choo , Hongwei Li , Ximeng Liu , Xiangdong Meng, Robert H. Deng, “Time-controlled hierarchical multikeyword search over encrypted data in cloud-assisted IoT”, *IEEE Internet of Things Journal*, Vol. 9, No.13, pp. 11017-11029, July 2022.
 85. Siqi Ma, Juanru Li, Surya Nepal, Diethelm Ostry, David Lo, Sanjay K. Jha, Robert H. Deng, Elisa Bertino, “Orchestration or automation: authentication flaw detection in Android apps”, *IEEE Transactions on Dependable and Secure Computing*, Vol 19, No. 4, pp. 2165-2178, Jul-Aug 2022.
 86. Willy Susilo, Peng Jiang, Jianchang Lai, Fuchun Guo, Guomin Yang, Robert H. Deng, “Sanitizable access control system for secure cloud storage against malicious data publishers”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 3, pp. 2138-2148, May-Jun 2022.
 87. Yinbin Miao, Qiuyun Tong, Robert H. Deng, Kim-Kwang Raymond Choo, Ximeng Liu, Hongwei Li, “Verifiable searchable encryption framework against insider keyword-guessing attack in cloud storage”, *IEEE Transactions on Cloud Computing*, Vol. 10, No. 2, pp. 835-848, Apr-Jun 2022.
 88. Guowen Xu, Hongwei Li, Yun Zhang, Shengmin Xu, Jianting Ning, Robert H. Deng, “Privacy-preserving federated deep learning with irregular users”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 2, pp. 1364-1381, Mar-Apr 2022.
 89. Jianting Ning, Geong Sen Poh, Xinyi Huang, Robert H. Deng, Shuwei Cao, Ee-Chien Chang, “Update recovery attacks on encrypted database within two updates using range queries leakage”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 2, pp. 1164-1180, Mar-Apr 2022.
 90. Jiayun Xu, Yingjiu Li, Robert H. Deng, Ke Xu, “SDAC: a slow-aging solution for Android malware detection using semantic distance based API clustering”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 2, pp. 1149-1163, Mar-Apr 2022.
 91. Shengmin Xu, Jianting Ning, Yingjiu Li, Yinghui Zhang, Guowen Xu, Xinyi Huang, Robert H. Deng, “Match in mw Way: fine-grained bilateral access control for secure cloud-fog computing”, *IEEE Transactions on Dependable and Secure Computing*, Vo. 19, No. 2, pp. 1064-1077, Mar-Apr 2022.

92. Zhuoran Ma, Jianfeng Ma, Yinbin Miao, Ximeng Liu, Kim-Kwang Raymond Choo, Yu Gao, Robert H. Deng, “Verifiable data mining against malicious adversaries in industrial Internet of Things”, *IEEE Transactions on Industrial Informatics*, Vol. 18, No. 2, pp. 953-964, Feb. 2022.
93. Shengmin Xu, Yingjiu Li, Robert H. Deng, Yinghui Zhang, Xiangyang Luo, Ximeng Liu, “Lightweight and expressive fine-grained access control for healthcare Internet-of-Things,” *IEEE Transactions on Cloud Computing*, Vol. 10, No. 1, pp. 474-490, Jan-Mar 2022.
94. Jinhua Ma, Xinyi Huang, Yi Mu, Robert H. Deng, “Authenticated data redaction with accountability and transparency”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 1, pp. 149-160, Jan-Feb 2022.
95. Haoran Yuan, Xiaofeng Chen, Jin Li, Tao Jiang, Jianfeng Wang, Robert H. Deng, “Secure cloud data deduplication with efficient re-encryption”, *IEEE Transactions on Service Computing*, Vol. 15, No. 1, pp. 442-456, Jan-Feb 2022.
96. Shengmin Xu, Jianting Ning, Xinyi Huang, Jianying Zhou, Robert H. Deng, “Server-aided bilateral access control for secure data sharing with dynamic user groups”, *IEEE Transactions Information Forensics and Security*, Vol. 16, pp. 4746-4761, Sept. 2021.
97. Yang Yang, Zhangshuang Guan, Zhiguo Wan, Jian Weng, HweeHwa Pang, Robert H. Deng, “PriScore: blockchain-based self-tallying election system supporting score voting”, *IEEE Transaction on Information Forensics and Security*, Vol. 16, pp. 4705-4720, Sept. 2021.
98. Zhenzhu Chen, Anmin Fu, Robert H. Deng, Ximeng Liu, Yang Yang, Yinghui Zhang, “Secure and verifiable outsourced data dimension reduction on dynamic data”, *Information Sciences*, Vol. 573, pp. 182-193, Sept. 2021.
99. Shengmin Xu, Jianting Ning, Jinhua Ma, Xinyi Huang, Robert H. Deng, “K-time modifiable and epoch-based redactable blockchain”, *IEEE Transactions on Information Forensics and Security*, Vol. 16, pp. 4507 – 4520, August 2021.
100. Pengfei Wu, Robert H. Deng, Qingni Shen, Ximeng Liu, Qi Li, Zhonghai Wu, “ObliComm: towards building an efficient oblivious communication system”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 5, pp. 2331-2348, Sept.-Oct. 2021.
101. Yinghui Zhang, Robert H. Deng, Ximeng Liu, and Dong Zheng, “Outsourcing service fair payment based on blockchain and its applications in cloud computing”, *IEEE Transactions on Services Computing*, Vol. 14, No. 4, pp. 1152-1166, July-Aug. 2021.
102. Yinbin Miao, Robert H. Deng, Raymond Choo, Ximeng Liu, Jianting Ning, and Hongwei Li, “Optimized verifiable fine-grained keyword search in dynamic multi-owner settings”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 4, pp. 1804-1820, July-Aug. 2021.
103. Yinbin Miao, Robert H. Deng, Ximeng Liu, Raymond Choo, Hongjun Wu, Hongwei Li, “Multi-authority attribute-based keyword search over encrypted cloud data”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 4, pp. 1667-1680, July-Aug. 2021.
104. Yinbin Miao, Ximeng Liu, Kim-Kwang Raymond Choo, Robert H. Deng, Jiguo Li, Hongwei Li, Jian-Feng Ma, “Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting.” *IEEE Transactions on Dependable Secure Computing*, Vol. 18, No. 3, pp. 1080-1094, May - June 2021.
105. Yangguang Tian, Yingjiu Li, Robert H. Deng, Binanda Sengupta, Guomin Yang, “Lattice-

- based remote user authentication from reusable fuzzy signature”, *Journal of Computer Security*, Vol. 29, No. 3, pp. 273-298, May – June 2021
106. Yinghui Zhang, Robert H. Deng, Elisa Bertino, Dong Zheng, “Robust and universal seamless handover authentication in 5G HetNets”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 2, pp. 858-874, Mar – Apr 2021.
 107. Yue Zhang, Jian Weng, Jia-Si Weng, Lin Hou, Anjia Yang, Ming Li, Yang Xiang, Robert H. Deng, “Looking back! Using early versions of Android apps as attack vectors”, *IEEE Transactions on Dependable Secure and Computing*, Vol. 18, No. 2, pp. 652-666, Mar – Apr 2021.
 108. Zhenzhu Chen, Anmin Fu, Yinghui Zhang, Zhe Liu, Fanjian Zeng and Robert H. Deng, "Secure Collaborative Deep Learning Against GAN Attacks in the Internet of Things," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5839-5849, 1 April, 2021
 109. Xueqin Liang, Zheng Yan, Robert H. Deng, Qinghua Zheng, “Investigating the adoption of hybrid encrypted cloud data deduplication with game theory”, *IEEE Transactions on Parallel and Distributed Systems*, Vol. 32, No. 3, pp. 587-600, March 2021.
 110. Tong Wu, Guomin Yang, Yi Mu, Fuchun Guo, and Robert H. Deng, “Privacy-preserving proof of storage for the pay-as-you-go business model”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 2, pp. 563-575, Mar - Apr 2021.
 111. Yan Li, Yao Cheng, Weizhi Meng, Yingjiu Li, Robert H. Deng, “Designing leakage-resilient password entry on head-mounted smart wearable glass devices”, *IEEE Transactions on Information Forensics and Security*, Vol. 16, pp. 307-321, 30 July 2021.
 112. Ximeng Liu, Robert H. Deng, Kim-Kwang Raymond Choo, Yang Yang, “Privacy-preserving outsourced clinical decision support system in the cloud”, *IEEE Transactions Service Computing*, Vol. 14, No. 1, pp. 222-234, Jan-Feb. 2021.
 113. Jiangang Shu, Kan Yang, Xiaohua Jia, Ximeng Liu, Cong Wang, Robert H. Deng, “Proxy-free privacy-preserving task matching with efficient revocation in crowdsourcing,” *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 1, pp.117-130, Jan – Feb 2021.
 114. Ximeng Liu, Robert H. Deng, Raymond Choo, and Yang Yang, “Privacy-preserving reinforcement learning design for patient-centric dynamic treatment regimes”, *IEEE Transactions on Emerging Topics in Computing*, Vol. 9, No. 1, pp. 456-470, Jan-Mar 2021.
 115. Qiu-Hong Wang, Steven M. Miller, Robert H. Deng, “Driving cybersecurity policy insights from information on the Internet”, *IEEE Security & Privacy*, Vo. 18, No. 6, pp. 42-50, Dec. 2020.
 116. Xueqiao Liu, Guomin Yang, Yi Mu, and Robert H. Deng, “Multi-user verifiable searchable symmetric encryption for cloud storage”, *IEEE Transactions on Dependable and Secure Computation*, Vol. 17, No. 6, pp. 1322-1332, Nov/Dec 2020.
 117. Jianfei Sun, Hu Xiong, Shufan Zhang, Ximeng Liu, Jiaming Yuan, Robert H. Deng, “Secure flexible and tampering-resistant data sharing system for vehicular social networks”, *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 11, pp. 12938 – 12950, Nov. 2020.
 118. Yangguang Tian, Yingjiu Li, Robert H. Deng, Nan Li, Pengfei Wu, Anyi Liu, “A new framework for privacy-preserving biometric-based remote user authentication”, *Journal of Computer Security*, Vol 28, No. 4, pp. 469-498, Sept/Oct 2020.
 119. Yinghui Zhang, Robert H. Deng, Shengmin Xu, Jianfei Sun, Qi Li, Dong Zheng, “Attribute-

- based encryption for cloud computing access control: a survey”, *ACM Computing Survey*, Vol. 53, No. 4, pp. 83:1-83:41, Sept 2020.
120. Ximeng Liu, Robert H. Deng, Kim-Kwang Raymond Choo, Yang Yang, HweeHwa Pang, “Privacy-preserving outsourced calculation toolkit in the cloud,” *IEEE Trans. Dependable Secure Computing*, 17, No. 5, pp. 898-911, Sept/Oct 2020.
 121. Jianfei Sun, Hu Xiong, Ximeng Liu, Yinghui Zhang, Xuyun Nie, Robert H. Deng, “Lightweight and privacy-aware fine-grained access control for IoT-oriented smart health”, *IEEE Internet Things J.* Vol 7, No. 7, pp. 6566-6575, July 2020.
 122. Binanda Sengupta, Yingjiu Li, Yangguang Tian, Robert H. Deng, “Editing-enabled signatures: a new tool for editing authenticated data”, *IEEE Internet Things J.* Vol. 7, No. 6, pp. 4997-5007, June 2020.
 123. Yujue Wang, HweeHwa Pang, Robert H. Deng, Yong Ding, Qianhong Wu, Bo Qin, Kefeng Fan, “Secure server-aided data sharing clique with attestation”, *Information Sciences*, Vol. 522, pp. 80-98, June 2020.
 124. Yang Yang, Ximeng Liu, Robert H. Deng, Jian Weng, “Flexible wildcard searchable encryption system”, *IEEE Transactions on Services Computing*, Vol. 13, No. 3, pp. 464-477, May/June 2020.
 125. Ximeng Liu, Robert H. Deng, Kim-Kwang Raymond Choo, Yang Yang, “Privacy-preserving outsourced support vector machine design for secure drug discovery”, *IEEE Trans. Cloud Computing*, Vol. 8, No. 2, pp. 610-622, Apr/Jun 2020.
 126. Hui Cui, Robert H. Deng, Baodong Qin, Jian Weng, “Key regeneration-free ciphertext-policy attribute-based encryption and its application”, *Information Sciences*, Vol. 517, pp. 217-229, May 2020.
 127. Hua Deng, Zheng Qin, Qianhong Wu, Zhenyu Guan, Robert H. Deng, Yujue Wang, Yunya Zhou, “Identity-based encryption transformation for flexible sharing of encrypted data in public cloud”, *IEEE Trans. Inf. Forensics Security*, Vol. 15, pp. 3168-3180, April 2020.
 128. Yang Yang, Ximeng Liu, Robert H. Deng, “Multi-user multi-keyword rank search over encrypted data in arbitrary language”, *IEEE Trans. Dependable Secure Computing*, Vol. 17, No. 2, pp. 320-334, Mar/Apr 2020.
 129. Wenxiu Ding, Zheng Yan and Robert H. Deng, “Privacy-preserving data processing with flexible access control”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 17, No. 2, pp. 363-376, Mar/Apr 2020.
 130. Binanda Sengupta, Yingjiu Li, Kai Bu, Robert H. Deng, “Privacy-preserving network path validation”, *ACM Trans. Internet Technology*, Vol. 20, No. 1, pp. 5:1-5:27, March 2020
 131. Yang Yang, Ximeng Liu, Robert H. Deng and Yingjiu Li, “Lightweight sharable and traceable secure mobile health system”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 17, No. 1, pp. 78-91, Jan/Feb 2020.
 132. Lin Liu, Jinshu Su, Ximeng Liu, Rongmao Chen, Kai Huang, Robert H. Deng, and Xiaofeng Wang, “Toward Highly Secure Yet Efficient KNN Classification Scheme on Outsourced Cloud Data”, *IEEE Internet of Things Journal*, Vol. 6, No. 6, pp. 9841-9852, December 2019.
 133. Guowen Xu, Hongwei Li, Hao Ren, Kan Yang, Robert H Deng, “Data security issues in deep learning: attacks, countermeasures, and opportunities”, *IEEE Communications Magazine*, Vol. 57, No. 11, pp. 116-122, November 2019.
 134. Yinghui Zhang, Robert H. Deng, Dong Zheng, Jin Li, Pengfei Wu, Jin Cao, “Efficient and robust certificateless signature for data crowdsensing in cloud-assisted industrial IoT”, *IEEE Transactions Industrial Informatics*, Vol. 15, No. 9, pp. 5099-5108, September 2019.

135. Yujue Wang, HweeHwa Pang, Robert H. Deng, Yong Ding, Qianhong Wu, Bo Qin, "Securing messaging services through efficient signcryption with designated equality test", *Information Sciences*, Vol. 490, pp. 146-165, July 2019.
136. Ming Li, Jian Weng, Anjia Yang, Wei Lu, Yue Zhang, Lin Hou, Jia-Nan Liu, Yang Xiang, Robert H. Deng, "CrowdBC: a blockchain-based decentralized framework for crowdsourcing", *IEEE Transactions on Parallel Distributed Systems*, Vol. 30, No. 6, pp. 1251-1266, June 2019.
137. Yinbin Miao, Qiuyun Tong, Kim-Kwang Raymond Choo, Ximeng Liu, Robert H Deng, Hongwei Li, "Secure online/offline data sharing framework for cloud-assisted industrial internet of things", *IEEE Internet of Things Journal*, Vol. 6, No. 5, pp. 8681-8691, June 2019.
138. Xingjie Yu, Michael Thang Shiwen, Yingjiu Li, Robert Huijie Deng, "Collusion attacks and fair time-locked deposits for fast-payment transactions in Bitcoin", *Journal of Computer Security*, Vol. 27, No. 3, pp. 375-403, June 2019.
139. Yinbin Miao, Ximeng Liu, Robert H. Deng, Hongjun Wu, Hongwei Li, Jiguo Li, Dapeng Wu, "Hybrid keyword-field search with efficient key management for industrial Internet of Things", *IEEE Trans. Industrial Informatics*, Vol. 15, No. 6, pp. 3206-3217, June 2019.
140. Mengmeng Yang, Tianqing Zhu, Kaitai Liang, Wanlei Zhou, Robert H Deng, "A blockchain-based location privacy-preserving crowdsensing system", *Future Generation Computer Systems*, Vol. 94, pp. 408-418, May 2019.
141. Yinbin Miao, Ximeng Liu, Kim-Kwang Raymond Choo, Robert H. Deng, Hongjun Wu, Hongwei Li, "Fair and dynamic data sharing framework in cloud-assisted Internet of Everything", *IEEE Internet of Things*, Vol. 6, No. 4, pp. 7201-7212, April 2019.
142. Hui Cui, Robert H. Deng, Yingjiu Li, Guowei Wu, "Attribute-based storage supporting secure deduplication of encrypted data in cloud," *IEEE Transactions on Big Data*, Vol. 5, No. 3, pp. 330-342, March 2019.
143. Jiangang Shu, Ximeng Liu, Kan Yang, Yinghui Zhang, Xiaohua Jia, Robert H. Deng, "SybSub: privacy-preserving expressive task subscription with sybil detection in crowdsourcing", *IEEE Internet of Things*, Vol. 6, No. 2, pp. 3003-3013, February 2019.
144. Yongdong Wu, Dengpan Ye, Zhuo Wei, Qian Wang, William Tan, Robert H. Deng, "Situation-aware authenticated video broadcasting over train-trackside WiFi networks", *IEEE Internet of Things*, Vol. 6, No. 2, pp. 1617-1627, February 2019.
145. Hui Cui, Robert H. Deng, and Guilin Wang, "An attribute-based framework for secure communications in vehicular ad hoc networks", *IEEE/ACM Transactions on Networking*, Vol. 27, No. 2, pp. 721-733, February 2019.
146. Ximing Liu, Yingjiu Li, Robert H. Deng, Bing Chang, and Shujun Li, "When human cognitive modeling meets PINs: user-independent inter-keystroke timing attacks", *Computer & Security*, Vol. 80, pp. 90-107, Jan. 2019.
147. Yinghui Zhang, Robert H. Deng, Gang Han, and Dong Zheng, "Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things", *Journal of Network and Computer Applications*, Vol. 123, pp. 89-100, December 2018.
148. Zhiguo Wan and Robert H. Deng, "VPSearch: achieving verifiability for privacy-preserving multi-keyword search over encrypted cloud data", *IEEE Transactions on Dependable and Secure Computing*, Vol. 15, No. 6, pp. 1083-1095, November/December, 2018.
149. Yinghui Zhang, Robert H. Deng, Jiangang Shu, Kan Yang, Dong Zheng, "TKSE: trustworthy

- keyword search over encrypted data with two-side verifiability via blockchain”, *IEEE Access*, Vol. 6, pp. 31077-31087, 2018.
150. Yinghui Zhang, Robert H. Deng, Ximeng Liu, Dong Zheng, “Blockchain based efficient and robust fair payment for outsourcing services in cloud computing”, *Information Sciences*, Vol. 462, pp. 262-277, Sept. 2018.
 151. Yongdong Wu, Zhuo Wei, Jian Weng, Xin Li, and Robert H. Deng, “Resonance attacks on load frequency control of smart grids”, *IEEE Transactions on Smart Grid*, Vol. 9, No. 5, pp. 4490-4502, Sept. 2018.
 152. Yang Yang, Ximeng Liu and Robert H. Deng, “Lightweight break-glass access control system for healthcare internet-of-things”, *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 8, pp. 3610-3617, Aug. 2018.
 153. Hui Cui, Robert H. Deng, Joseph K. Liu, Xun Yi, Yingjiu Li, “Server-aided attribute-based signature with revocation for resource-constrained industrial-Internet-of-Things devices”, *IEEE Transactions on Industrial Informatics*, Vol. 14, No. 8, pp. 3724-3732, Aug. 2018.
 154. Jiangang Shu, Ximeng Liu, Xiaohua Jia, Kan Yang, Robert H. Deng, “Anonymous privacy-preserving task matching in crowdsourcing”, *IEEE Internet of Things Journal*, Vol. 5, No. 4, pp. 3068-3078, August 2018.
 155. Shengmin Xu, Guomin Yang, Yi Mu, Robert H. Deng, “Secure fine-grained access control and data sharing for dynamic groups in the cloud”, *IEEE Trans. Information Forensics and Security*, Vol. 13, No. 8, pp. 2101-2113, Aug. 2018.
 156. Yongdong Wu, Zhuo Wei, Jian Weng, and Robert H. Deng, “Position manipulation attacks to balise-based train automatic stop control”, *IEEE Transactions on Vehicular Technology*, Vol. 67, No. 6, pp. 5287-2301, June 2018.
 157. Yinghui Zhang, Dong Zheng, Robert H. Deng, “Security and privacy in smart health: efficient policy-hiding attribute-based access control”, *IEEE Internet of Things Journal*, Vol. 5, No. 3, pp. 2130-2145, June 2018.(IF 7.586 as of June 2018)
 158. Yujue Wang, HweeHwa Pang, Robert H. Deng, “Verifiably encrypted cascade-instantiable blank signatures to secure progress decision management”, *International Journal of Information Security*, Springer, Vol. 17, No. 3, pp. 347-363, June 2018
 159. Hui Cui, Zhiguo Wan, Robert H. Deng, Guilin Wang, and Yingjiu Li, “Efficient and expressive keyword search over encrypted data in the cloud”, *IEEE Transactions on Secure and Dependable Secure Computing*, Vol. 15, No. 3, pp. 409-422, May/June 2018.
 160. Yang Yang, Ximeng Liu, Robert H. Deng, “Expressive query over outsourced encrypted data”, *Information Science*, Vol. 442-443, pp. 33-53, May 2018.
 161. Yan Li, Yingjiu Li, Ke Xu, Qiang Yan, and Robert H. Deng, “Empirical study of face authentication systems under OSNFD attacks”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 15, No. 2, pp. 231-245, March/April 2018.
 162. Hui Cui, Robert H. Deng, Junzuo Lai, Xun Yi, Surya Nepal, “An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited”, *Computer Networks*, Vol. 133, pp. 157-165, March 2018
 163. Hui Cui, Robert H. Deng, Yingjiu Li, “Attribute-based cloud storage with secure provenance over encrypted data”, *Future Generation Computer Systems*, vol. 79, no. 2, pp. 461-472, Feb 2018
 164. Ximeng Liu, Raymond Choo, Robert H. Deng, Rongxing Lu and Jian Weng, “Efficient and

- privacy-preserving outsourced calculation of rational numbers”, *IEEE Transactions on Dependable and Secure Computing*, Vol. 15, No. 1, pp. 27-29, January/February 2018.
165. Ximeng Liu, Robert H. Deng, Yang Yang, Ngoc Hieu Tran, and Shangping Zhong, “Hybrid privacy-preserving clinical decision support system in fog-cloud computing”, *Future Generation Computing Systems*, Vol. 78, Part 1, pp. 825-837, Jan. 2018.
 166. Dong Shen, Zhoujun Li, Xiaojing Su, Jinxin Ma, Robert Huijie Deng, “TinyVisor: An extensible secure framework on android platforms”, *Computers & Security*, Vol. 72, pp. 145-162, Jan. 2018.
 167. Yujue Wang, Hwee Hwa Pang, Ngoc Hieu Tran and Robert H. Deng, “CCA secure encryption supporting authorized equality test on ciphertexts in standard model and its applications”, *Information Sciences*, Vol. 414, pp. 289-305, Elsevier, November 2017.
 168. Wenxiu Ding, Zheng Yan, and Robert H. Deng, “Encrypted data processing with homomorphic re-encryption”, *Information Sciences*, Elsevier, Vol. 409, pp. 35-55, October 2017.
 169. Siqi Ma, Junzuo Lai, Robert H Deng, Xuhua Ding, “Adaptable key-policy attribute-based encryption with time interval”, *Soft Computing*, Vol. 21, No. 20, pp. 6191-6200, October 2017.
 170. Dong Shen, Zhoujun Li, Xiaojing Su, Jinxin Ma, and Robert H. Deng, “TinyVisor: an extensible secure framework on Android platforms”, *Computers and Security*, Vol. 72, pp. 145-162, Sept 2017, Elsevier.
 171. Baodong Qin, Shengli Liu, Shifeng Sun, Robert H. Deng, Dawu Gu, “Related-key secure key encapsulation from extended computational bilinear Diffie–Hellman”, *Information Sciences*, Elsevier, Vol. 406, pp. 1-11, September 2017.
 172. Ximeng Liu, Baodong Qin, Robert H. Deng, Yingjiu Li, “An efficient privacy-preserving outsourced computation over public data”, *IEEE Transactions on Services Computing*, Vol. 10, No. 5, pp. 756-770, Sept/Oct 2017.
 173. Zhuo Wei, Yanjiang Yang, Yongdong Wu, Jian Weng, Robert H. Deng, “HIBS-KSharing: hierarchical identity-based signature key sharing for automotive”, *IEEE Access* Vol. 5, pp. 16314-16323, August 2017
 174. Daibin Wang, Haixia Yao, Yingjiu Li, Hai Jin, Deqing Zou, Robert H. Deng, “A secure, usable, and transparent middleware for permission managers on Android”, *IEEE Transactions on Dependable and Secure Computing*, vol. 14, No. 4, pp. 350-362, July/August 2017.
 175. Yao Cheng, Yingjiu Li, Robert Deng, Lingyun Ying, Wei He, “A study on a feasible no-root approach on Android”, *Journal of Computer Security*, Vol. 25, No. 3, pp. 231-253, June 2017.
 176. Yujue Wang, Qianhong Wu, Bo Qin; Wenchang Shi, Robert H. Deng and Jiankun Hu, “Identity-based data outsourcing with comprehensive auditing in clouds”, *IEEE Transactions on Information Forensic and Security*, Vol. 12, No. 4, pp. 940-952, April 2017.
 177. Yongdong Wu, Jian Weng, Zhe Tang, Xin Li and Robert H. Deng, “Vulnerabilities, attacks and countermeasures in balise-based train control systems”, *IEEE Transactions on Intelligent Transportation Systems*, Vol. 18, No. 4, pp. 814-823, April 2017.
 178. Chunhua Su, Bagus Santoso, Yingjiu Li, Robert H. Deng, and Xinyi Huang, “Universally composable RFID mutual authentication”, *IEEE Transactions on Secure and Dependable Computing*, Vol. 14, No. 1, pp. 83-94, Jan/Feb 2017.
 179. Lixian Liu, Junzuo Lai, Robert H Deng, Yingjiu Li, “Ciphertext-policy attribute-based

- encryption with partially hidden access structure and its application to privacy-preserving electronic medical record system in cloud environment”, *Security and Communication Networks*, Vol. 9, No. 18, pp. 4897-4913, December 2016.
180. Zhuo Wei, Zheng Yan, Yongdong Wu, and Robert H. Deng, “Trustworthy authentication on scalable surveillance video with background model support”, *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, Vol. 12, No. 4s, pp. 1-20, November 2016.
 181. Hui Cui, Guilin Wang, Robert H. Deng, and Baodong Qin, “Escrow free attribute-based signature with self-revealability”, *Information Sciences*, Vol. 367, No. C, pp. 660-672, November 2016.
 182. Kai He, Jian Weng, Robert H. Deng, Joseph K. Liu, “On the security of two identity-based conditional proxy re-encryption schemes”, *Theoretical Computer Science*, Vol. 652, pp. 18-27, Nov. 2016
 183. Ximeng Liu, Robert H. Deng, Wenxiu Ding, Rongxing Lu, and Baodong Qin, “Privacy-preserving outsourced calculation on floating point numbers”, *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 11, pp. 2513 – 2527, November 2016.
 184. Ximeng Liu, Robert H. Deng, Raymond Choo, Jian Weng, “An efficient privacy-preserving outsourced calculation toolkits with multiple keys”, *IEEE Transactions on Information Forensics and Security*, Vol. 11, No. 11, pp. 2401-2414, November 2016
 185. Hui Cui and Robert H. Deng, “Revocable and decentralized attribute-based encryption”, *The Computer Journal*, Vol. 59, No. 8, pp. 1220-1235, August 2016.
 186. Wenxiu Ding, Zheng Yan, and Robert H. Deng, “A survey on future internet security architectures”, *IEEE Access*, Vol. 4, pp. 4374-4393, 29 July 2016.
 187. Ke Xu, Yingjiu Li, and Robert H. Deng, “ICCDetector: ICC-Based Malware Detection on Android”, *IEEE Transactions on Information Forensics & Security*, Vol. 11, No. 6, pp. 1252-1264, June 2016.
 188. Zheng Yan, Wenxiu Ding, Xixun Yu, Haiqi Zhu, Robert H. Deng, “Deduplication on encrypted big data in cloud”, *IEEE Transactions on Big Data*, Vol. 2, No. 2, pp. 138-150, July, 2016.
 189. Ximeng Liu, Baodong Qin, Robert H. Deng, Rongxing Lu and Jianfeng Ma, “A privacy-preserving outsourced functional computation framework across large-scale multiple encrypted domains”, *IEEE Transactions on Computers*, Vol. 65, No. 12, pp. 3567-3579, Dec. 2016.
 190. Jialie Shen, Robert H. Deng, Zhiyong Cheng, Liqiang Nie, and Shuicheng Yan, “On robust image spam filtering via comprehensive visual modeling”, *Pattern Recognition*, Elsevier, Vol. 48, No., 10, pp. 3227-3238, October 2015.
 191. Jian Weng, Yunlei Zhao, Robert H. Deng, Shengli Liu, Yanjiang Yang, Kouichi Sakurai, “A note on the security of KHL scheme”, *Theoretical Computer Science*, Elsevier, Vol. 602, pp. 1-6, October 2015.
 192. Baodong Qin, Robert H. Deng, Shengli Liu, and Siqi Ma, “Attribute-based encryption with efficient verifiable outsourced decryption”, *IEEE Transactions on Secure and Dependable Computing*, Vol. 10, No. 7, pp. 1384-1393, July 2015.
 193. Yinxia Sun, Futai Zhang, Limin Shen and Robert H. Deng, “Efficient revocable certificateless encryption against decryption key exposure”, *IET Information Security*, Vol. 9, No. 3, pp. 158-

166, May 2015.

194. Yan Li, Yingjiu Li, Qiang Yan and Robert H. Deng, "Privacy leakage analysis in online social networks", *Computers & Security*, Vol. 49, pp. 239-254. Elsevier, March 2015.
195. Qiang Yan, Jin Han, Yingjiu Li, Jianying Zhou, Robert H. Deng, "Leakage-resilient password entry: challenges, design, and evaluation", *Computers & Security*, Elsevier, Vol. 48, pp. 196-211, February 2015.
196. Yongdong Wu, Zhigang Zhao, Feng Bao and Robert H. Deng, "Software puzzle: a countermeasure to resource-inflated denial-of-service attacks", *IEEE Transactions on Information Forensics & Security*, Vol. 10, No. 1, pp. 168-177, January 2015.
197. Junzuo Lai, Yingjiu Li, Robert H. Deng, Qiang Yan, Jian Weng and Chaowen Guan, "Towards semantically secure outsourcing of association rule mining on categorical data", *Information Sciences*, Vol. 267, pp. 267-286, May 2014.
198. Yifan Zhao, Swee-Won Lo, Robert H. Deng and Xuhua Ding, "Technique for authenticating H.264/SVC and its performance evaluation over wireless mobile networks", *Journal of Computer and System Sciences*, Vol. 80, No. 3, pp. 520-532, Elsevier, May 2014.
199. Zhuo Wei, Yongdong Wu, Robert H. Deng and Xuhua Ding, "A hybrid scheme for authenticating scalable video codestreams", *IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 4, pp. 543-553, April 2014.
200. Robert H. Deng, Xuhua Ding and Swee-Won Lo, "Efficient authentication and access control of scalable multimedia streams over packet-lossy networks", *Journal of Security and Communication Networks*, Vol. 7, No. 3, pp. 611-625, March 2014.
201. Robert H. Deng, Xuhua Ding, Yongdong Wu and Zhuo Wei, "Efficient block-based transparent encryption for H.264/SVC bitstreams", *Multimedia Systems*, Vol. 20, No. 2, pp. 165-178, February 2014.
202. Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying and Robert H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 25, No. 2, pp. 468-477, February 2014.
203. Yueqiang Cheng, Xuhua Ding and Robert H. Deng, "DriverGuard: virtualization based fine-grained protection on I/O flows", *ACM Transactions on Information and System Security*, Vol. 16, No. 2, pp. 6.1 – 6.30, September 2013.
204. Zhiguo Wan, Jun'e Liu, Rui Zhang, Robert H. Deng, "A collusion-resistant conditional access system for flexible-pay-per-channel pay-TV broadcasting", *IEEE Transactions on Multimedia*, Vol. 15, No. 6, pp. 1353-1364, October 2013.
205. Junzuo Lai, Robert H. Deng, Chaowen Guan and Jian Weng, "Attributed-based encryption with verifiable outsourced decryption", *IEEE Transactions on Information Forensics and Security*, Vol. 8, No. 8, pp. 1343-1354, August 2013.
206. Yongdong Wu, Zhuo Wei and Robert H. Deng, "Attributed-based access to scalable media in cloud-assisted content sharing", *IEEE Transactions on Multimedia*, Vol. 15, No. 4, pp. 778-788, June 2013.
207. Jie Shi, Yingjiu Li and Robert H. Deng, "A secure and efficient discovery service system in EPCglobal network", *Computer & Security*, Vol. 31, No. 8, Elsevier, pp. 870-885, November 2012.
208. Wen Tao Zhu, Jianying Zhou, Robert H. Deng and Feng Bao, "Detecting node replication attacks in mobile sensor networks: theory and approaches", *Security and Communication*

Networks, Vol. 5, No. 5, pp. pp. 496-507, Wiley InterScience, 2012.

209. Xinyi Huang, Cheng-Keng Chu, Hung-Min Sun, Jianying Zhou, and Robert H. Deng, "Enhanced authentication for commercial video services", *Journal of Security and Communication Networks*, Vol. 5, No. 11, pp. 1248-1259, November 2012.
210. Zhuo Wei, Yongdong Wu, Xuhua Ding and Robert H. Deng, "A scalable and format-compliant encryption scheme for H.264/SVC bitstreams", *Signal Processing: Image Communication*, Vol. 27, No. 9, pp. 1011-1024, Elsevier, October 2012.
211. Wen Tao Zhu, Jianying Zhou, Robert H. Deng and Feng Bao, "Detecting node replication attacks in wireless sensor networks: a survey", *Journal of Network and Computer Applications*, Vol. 35, No. 3, pp. 1022-1034, May 2012.
212. Zhiguo Wan, Jun'e Liu and Robert H. Deng, "HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing", *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 2, pp.743-754, April 2012.
213. Yingjiu Li, Robert H. Deng, Junzuo Lai, Tieyan Li and Changshe Ma, "On two RFID privacy notions and their relations", *ACM Transactions on Information and System Security*, August Vol. 14, No. 4, pp. 30:1-23, 2011.
214. Xinyi Huang, Yang Xiang, Ashley Chonka, Jianying Zhou and Robert H. Deng, "A generic framework for three-factor authentication: preserving security and privacy in distributed systems", *IEEE Transactions on Parallel and Distributed Systems*, Vol. 22, No. 8, pp. 1390-1397, August 2011.
215. Robert H. Deng, Yingjiu Li, Moti Yung and Yunlei Zhao, "A zero-knowledge based framework for RFID privacy", *Journal of Computer Security*, Vol. 19, No. 6, pp. 1109-1146, 2011, IOS Press.
216. Wen Tao Zhu, Yang Xiang, Jianying Zhou, Robert H. Deng and Feng Bao, "Secure localization with attack detection in wireless sensor networks", *International Journal of Information Security*, Vol. 10, No. 3, pp. 155-171, June 2011.
217. Xinyi Huang, Yi Mu, Willy Susilo, Jianying Zhou and Robert H. Deng, "Preserving transparency and accountability in optimistic fair exchange of digital signatures", *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 2, pp. 498-512, June 2011.
218. Xuhua Ding, Yanjiang Yang, Robert H. Deng, "Database access pattern protection without full-shuffles", *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 1, pp. 189-201, March 2011.
219. Jian Weng, Guoxiang Yao, Robert H. Deng, Min-Rong Chen, Xiangxue Li, "Cryptanalysis of a certificateless signcryption scheme in the standard model", *Information Sciences*, Volume 181, Issue 3, pp. 661-667, 1 February 2011.
220. Yanjiang Yang, Jianying Zhou, Robert H. Deng and Feng Bao, "Better security enforcement in trusted computing enabled heterogeneous wireless sensor networks", *Journal of Security and Communication Networks*, Vol. 4, No. 1, pp. 11-22, Wiley InterScience, January 2011.
221. Jian Weng, Robert H. Deng, Shengli Liu and Keifei Chen, "Chosen-ciphertext secure bidirectional proxy re-encryption schemes without pairings", *Information Sciences*, Vol. 180, Issue 24, pp. 5077-5089, December 2010.
222. Yongdong Wu, Zhou Wei, Haixia Yao, Zhigang Zhao, Ngoh Lek Heng, Robert H. Deng, and Shengsheng Yu "TeleOph: a secure real-time teleophthalmology system", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 14, No. 5, pp. 1259-1266, September 2010.

223. Xuhua Ding, Yanjiang Yang, Robert H. Deng and Shuhong Wang "A new hardware-assisted PIR with $O(n)$ shuffle cost", *International Journal of Information Security*, Springer, Vol. 9, No. 4, pp. 237-252, August 2010.
224. Yanjiang Yang, Yingjiu Li, Robert H. Deng and Feng Bao, "Shifting Inference Control to User Side: Architecture and Protocol", *IEEE Transactions on Dependable and Secure Computing*, Vol. 7, No. 2, pp. 189-202, April-June 2010.
225. Changshe Ma, Jian Weng, Yingjiu Li and Robert H. Deng, "Efficient discrete logarithm based multi-signature scheme in the plain public key model", *Designs, Codes and Cryptography*, Vol. 54, No. 2, pp. 121-133, Springer, February 2010.
226. Yanjiang Yang, Robert H. Deng and Feng Bao, "Privacy-preserving rental services using one-show anonymous credentials", *Journal of Security and Communication Networks*, Vol. 2, No. 6, pp. 531-545, Wiley InterScience, November/December 2009.
227. Yanjiang Yang, Feng Bao, Xuhua Ding and Robert H. Deng, "Multiuser private queries over encrypted databases", *International Journal of Applied Cryptography*, Vol. 1, No. 4, pp. 309-319, Inderscience, 2009.
228. R. H. Deng and Y. Yang, "A study of data authentication in proxy-enabled multimedia delivery systems: model, schemes and application", *ACM Transactions on Multimedia Computing, Communications and Applications*, Vol. 5, No. 4, pp. 28.1-28.20, October 2009.
229. Zhuo Wei, Yongdong Wu, Robert H. Deng, Shengsheng Yu, Haixia Yao, Zhigang Zhao, Lek Heng Ngoh, Lim Tock Han, Eugenie Poh, "A secure and synthesis tele-ophthalmology system", *Journal of Telemedicine and e-Health*, American Telemedicine Association, Vol. 14, No. 8, pp. 833-845, October 2008.
230. T. Li, R. H. Deng and G. Wang, "The security and improvement of an ultra-lightweight RFID authentication protocol", *Journal of Security and Communication Networks*, Vol.1, No. 2, pp. 135-146, March/April 2008, Wiley InterScience.
231. Y. Wu, D. Ma and R. H. Deng, "Flexible access control to JPEG2000 image code-streams", *IEEE Transactions on Multimedia*, Vol. 9, No. 6, pp. 1314-1324, October 2007.
232. Z. Wan, R. H. Deng, F. Bao, A. L. Ananda, "Access control protocols with two-layer architecture for wireless networks", *Journal of Computer Network*, Vol. 51, No. 3, pp. 655-670, Feb. 2007.
233. S.-T. Goh, H. H. Pang, R. H. Deng and F. Bao, "Three architectures for trusted data dissemination in edge computing", *Data and Knowledge Engineering Journal*, Vol. 58, No. 3, pp. 381-409, September 2006.
234. K. Ren, W. Lou, K. Kim and R. H. Deng, "A novel privacy preserving authentication and access control scheme in pervasive computing environments", *IEEE Transactions on Vehicular Technology*, Vol. 55, No. 4, pp. 1373-1384, July 2006.
235. Z. Wan, F. Bao, R. H. Deng and A. L. Ananda, "Security analysis on a conference scheme for mobile communications", *IEEE Transactions on Wireless Communications*, Vol. 5, No. 6, pp. 1238-1240, June 2006.
236. D. Kwak, S. Moon, G. Wang and R. H. Deng, "A secure extension of the Kwak-Moon group signcryption scheme", *Journal of Computers & Security*, Vol. 25, No. 6, pp. 435-444, Elsevier, Sept. 2006.
237. K. Ren, W. Lou, K. Zeng, F. Bao, J. Zhou and R. H. Deng, "Routing optimization security in mobile IPv6", *Computer Networks Journal*, Vol. 50, No. 13, pp. 2401-2419, Elsevier, 2006.

238. Y. Yang, R. H. Deng and F. Bao, "A Practical Password-Based Two-Server Authentication and Key Exchange System", *IEEE Transactions on Dependable and Secure Computing*, Vol. 3, No. 2, pp. 105-114, April-June 2006.
239. Y. Wu and R. H. Deng, "Scalable authentication of MPEG-4 streams", *IEEE Transactions on Multimedia*, Vol. 8, No. 1, pp. 152-161, Feb. 2006.
240. J. Zhou, F. Bao and R. H. Deng, "Minimizing TTP's involvement in signature validation", *International Journal of Information Security*, Springer, Vol. 5, No. 1, pp. 37-47, January 2006
241. F. Bao, R. H. Deng, B. C. Ooi and Y. Yang, "Tailored reversible watermarking schemes for authentication of electronic clinical atlases", *IEEE Transactions on Information Technology in Biomedicine*, Vol. 9, No. 4, pp. 554-563, December 2005.
242. R. H. Deng, D. Ma, W. Shao and Y. Wu, "Scalable trusted online dissemination of JPEG2000 images", *ACM Multimedia Systems Journal*, Vol. 11, pp. 60-67, November 2005.
243. F. Bao and R. H. Deng, "Protocols that hide user's preferences in electronic transactions", *Journal of Computer Networks*, Vol. 48, No. 4, pp. 503-515, July 2005
244. B. Zhu, F. Bao, R. H. Deng, M. Kankanhalli and G. Wang, "Efficient and robust key management for large mobile ad-hoc networks", *Computer Networks Journal*, Vol. 48, No. 4, pp. 657-682, July 2004.
245. Y. Yang, S. Wang, F. Bao, J. Wang and R. H. Deng, "New efficient user identification and key distribution scheme providing enhanced security", *Computers & Security*, No. 12, pp. 3443-3346, Elsevier, Dec. 2004.
246. G. Wang, F. Bao, J. Zhou and R. H. Deng, "Comments on a threshold proxy signature scheme based on the RSA cryptosystem", *IEEE Transactions on Knowledge and Data Engineering*, Vol. 16, No. 11, pp. 1309-1311, October 2004.
247. K. Ren, T. Y. Li, Z. Wan, F. Bao, R. H. Deng and K. Kim, "Highly reliable trust establishment scheme in ad-hoc networks", *Computer Networks Journal*, Vol. 45, No. 6, pp. 687-699, Elsevier, 2004.
248. Y. Yang, X. Han, F. Bao and R. H. Deng, "A smart-card enabled privacy preserving e-prescription system", *IEEE Transactions on Information Technology in Biomedicine*, pp. Vol. 8, No. 1, pp. 47-58, March 2004.
249. J. Zhou and R. H. Deng, "On the validity of digital signatures", *ACM SIGCOMM Computer Communication Review*, Vol. 30, No. 2, pp. 29-34, ACM Press, April 2000.
250. X. Wang, R. H. Deng, F. Bao, "Multicast Internet Protocol", *Journal of Computer Communications*, Vol. 23, pp. 1047-1054, 2000.
251. R. H. Deng, L. Gong, A. A. Lazar, W. Wang, "Practical protocols for certified electronic mail," *Journal of Network and Systems Management*, Vol. 4, No. 3, pp. 279-297, 1996.
252. H. Zhou and R. H. Deng, "Type-I hybrid ARQ scheme with time diversity for binary digital FM cellular radio," *IEE Proceedings-Communications*, Vol. 143, No. 1, pp. 29-36, Feb. 1996.
253. R. H. Deng and M. L. Lin, "A type I hybrid ARQ system with adaptive code rates," *IEEE Transactions on Communications*, Vol. 43, No. 2/3/4, Feb/March/April 1995.
254. R. H. Deng, "Hybrid ARQ schemes employing coded modulation and sequence combining," *IEEE Transactions on Communications*, Vol. 42, No. 6, pp. 2239-2245, June 1994.
255. H. Zhou, R. H. Deng, and T. T. Tjhung, "Performance of combined diversity reception and convolutional coding for QPSK land mobile radio," *IEEE Transactions on Vehicular Technology*, Vol. 43, No. 3, pp. 499-508, August 1994.

256. K. S. Lim, R. H. Deng, and K. Ranai, "Exact and approximate models to obtain average throughput of the FDDI MAC protocol - part I: symmetric systems," *Journal of Computer Communications*, Vol. 17, No. 2, pp. 83-93, Feb. 1994.
257. K. S. Lim, R. H. Deng, and K. Ranai, "Exact and approximate models to obtain average throughput of the FDDI MAC protocol - part II: asymmetric systems," *Journal of Computer Communications*, Vol. 17, No. 4, pp. 251-256, April, 1994.
258. Y. X. Li, R. H. Deng, and X. M. Wang, "On the equivalence of McEliece's and Niederreiter's public-key cryptosystems," *IEEE Transactions on Information Theory*, Vol. 40, No. 1, pp. 271-273, January 1994.
259. J. Du, R. H. Deng, and C. C. Ko, "Performance analysis of interconnected LANs with server/client configuration," *Journal of Computer Networks and ISDN Systems*, Vol. 25, pp. 1321-1333, 1993
260. R. H. Deng, X. Y. Zhang, and K. T. Huang, "Performance of a token-passing system with batch arrivals and its applications to file transfers," *Journal of Computer Communications*, Vol. 16, No. 7, pp. 422-431, July 1993.
261. R. H. Deng, A. A. Lazar, and W. Wang, "A probabilistic approach to fault diagnosis in linear lightwave networks," *IEEE Journal of Selected Areas in Communications*, Vol. 11, No. 9, pp. 1438-1448, Dec. 1993.
262. R. H. Deng and R. Shu, "A LAN based medical image visualization system and its performance study," *Journal of Computer Communications*, Vol. 16, No. 8, pp. 518-525, August 1993.
263. R. H. Deng and H. Zhou, "An adaptive coding scheme with code combining for mobile radio systems," *IEEE Transactions on Vehicular Technology*, Vol. 42, No. 4, pp. 469-476, Nov. 1993.
264. R. H. Deng, "Hybrid ARQ schemes for point-to-multipoint communications over nonstationary broadcast channels," *IEEE Transactions on Communications*, Vol. 41, No. 9, pp. 1379-1387, Sept. 1993.
265. S. S. Pietrobon, R. H. Deng, A. LaFanechere, G. Ungerboeck, and D. J. Costello, Jr., "Trellis-coded multidimensional phase modulation," *IEEE Transactions on Information Theory*, Vol. 36, No. 1, pp. 63-89, January 1990.
266. X. Y. Zhang and R. H. Deng, "Gateway design for LAN interconnection via ISDN," *Journal of Computer Networks and ISDN Systems*, Vol. 19, pp. 43-51, Sept. 1990.
267. R. H. Deng and D. J. Costello, Jr., "High rate concatenated coding systems using bandwidth efficient trellis inner codes," *IEEE Transactions on Communications*, Vol. 37, No. 5, pp. 420-427, May 1989.
268. L. R. Lugand, D. J. Costello, Jr., and R. H. Deng, "Parity retransmission hybrid ARQ using rate 1/2 convolutional codes on a nonstationary channel," *IEEE Transactions on Communications*, Vol. 37, No. 7, pp. 755-765, July 1989.
269. R. H. Deng, X. Y. Zhang, and Y. K. Tham, "New point-to-multipoint communications protocols," *IEE Proceedings*, Vol. 136, Part I, No. 4, pp. 312-316, August 1989.
270. R. H. Deng and D. J. Costello, Jr., "High rate concatenated coding systems using multidimensional bandwidth efficient inner codes," *IEEE Transactions on Communications*, Vol. 37, No. 10, pp. 1091-1096, October 1989.

271. R. H. Deng and M. A. Herro, "DC-free coset codes," *IEEE Transactions on Information Theory*, Vol. 34, No. 4, pp. 786-792, July 1988.
272. R. H. Deng and D. J. Costello, Jr., "Decoding of DBEC-TBED Reed-Solomon codes," *IEEE Transactions on Computers*, Vol. 36, No. 11, pp. 1359-1363, Nov. 1987.
273. R. H. Deng and D. J. Costello, Jr., "Reliability and throughput analysis of a concatenated coding system," *IEEE Transactions on Communications*, Vol. 35, No. 7, pp. 698-705, July 1987.

Refereed Conference Proceedings Publications

1. Zhe Ren, Xinghua Li, Yinbin Miao, Mengyao Zhu, Shunjie Yuan, Robert H. Deng, "PIC-BI: Practical and intelligent combinatorial batch identification for UAV assisted IoT networks", *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2024)*, 14-18 October, 2024, Salt Lake City, USA
2. Zhikang Xie, Mengling Liu, Haiyang Xue, Man Ho Au, Robert H. Deng, Siu-Ming Yiu, "Direct range proofs for Paillier cryptosystem and their applications", *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2024)*, 14-18 October, 2024, Salt Lake City, USA
3. Xiaoguo Li, Guomin Yang, Tao Xiang, Bowen Zhao, HweeHwa Pang, Robert H. Deng, "Make revocation cheaper: hardware-based revocable attribute-based encryption", *Proceedings of IEEE Symposium on Security and Privacy (S&P 2024)*, pp. 3109-3127, 20-22 May 2024, San Francisco, USA.
4. Yang Yang, Robert H. Deng, Guomin Yang, Yingjiu Li, HweeHwa Pang, Minming Huang, Rui Shi, Jian Weng, "PriSrv: privacy-enhanced and highly usable service discovery in wireless communications", *Proceedings of the Network and Distributed System Security Symposium (NDSS 2024)*, 26 Feb – 1 Mar 2024, San Diego, USA.
5. Yinbin Miao, Chao Xu, Yifeng Zheng, Ximeng Liu, Xiangdong Meng, Robert H. Deng, "Efficient and Secure Spatial Range Query over Large-scale Encrypted Data", *Proceedings of the 43rd IEEE International Conference on Distributed Computing Systems (ICDCS 2023)*, pp. 1-11, 18-21 July 2023.
6. Wenxiu Ding, Wei Sun, Zheng Yan, Robert H. Deng, Zhiguo Wan "An efficient and secure scheme of verifiable computation for Intel SGX", *Proceedings of the 21st IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2022)*, pp. 473-482, 9-11 December 2022, Wuhan, China. **Outstanding Paper.**
7. Yinbin Miao, Rongpeng Xie, Xinghua Li, Ximeng Liu, Zhuo Ma, Robert H. Deng, "Communication efficient federated learning based on adaptive local differential privacy", *Proceedings of the 38th Annual Computer Security Applications Conference (ACSAC 2022)*, pp. 159-170, 5-9 December 2022, Austin, Texas, USA.
8. Jiaming Yuan, Yingjiu Li, Jianting Ning, Robert H. Deng, "M-EDESE: Multi-Domain, Easily Deployable, and Efficiently Searchable Encryption", *Proceedings of the 17th International Conference on Information Security Practice and Experience (ISPEC 2022)*, pp. 606-623, 23-25 November 2022, Taipei, Taiwan.
9. Yutao Yang, Yinbin Miao, Kim-Kwang Raymond Choo, Robert H. Deng, "Lightweight privacy-preserving spatial keyword query over encrypted cloud data", *Proceedings of the 42nd IEEE International Conference on Distributed Computing Systems (ICDCS 2022)*, pp. 392-

402, Bologna, Italy, July 10-13, 2022.

10. Bowen Zhao, Yingjiu Li, Ximeng Liu, Hwee Hwa Pang, Robert H. Deng, “FREED: An efficient privacy-preserving solution for person re-identification”, *Proceedings of the IEEE Conference on Dependable and Secure Computing (IEEE DSC 2022)*, pp. 1-8, 22-24 June 2022, Edinburgh, UK. **Best Paper Award**.
11. Shengmin Xu, Jianting Ning, Jinhua Ma, Guowen Xu, Jiaming Yuan, Robert H. Deng, “Revocable policy-based Chameleon hash”, *Proceedings of the 26th European Symposium on Research in Computer Security (ESORICS 2021)*, LNCS 12972, pp. 327-347, 4-8 October 2021, Online.
12. Jianting Ning, Xinyi Huang, Geong Sen Poh, Jiaming Yuan, Yingjiu Li, Jian Weng and Robert H. Deng, “LEAP: Leakage-Abuse Attack on Efficiently Deployable, Efficiently Searchable Encryption with Partially Known Dataset”, *Proceedings of the ACM Conference on Computer and Communications Security (ACM CCS 2021)*, 14-19 November 2021, online.
13. Shengmin Xu, Jianting Ning, Jinhua Ma, Xinyi Huang, Hwee Hwa Pang, Robert H. Deng, “Expressive bilateral access control for Internet-of-Things in cloud-fog computing” *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies (SACMAT 2021)*, pp. 143-154, 16-18 June 2021, Barcelona, Spain.
14. Daoyuan Wu, Debin Gao, Robert H. Deng and Rocky Chang, “When program analysis meets bytecode search: targeted and efficient inter-procedural analysis of modern Android apps in BackDroid”, *Proceedings of the 51st IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2021)*, pp. 543-554, 12-24 June 2021, Taipei. (AR 16.3%).
15. Ximing Liu, Yingjiu Li, and Robert H. Deng, “UltraPIN: inferring PIN entries via ultrasound”, *Proceedings of the ACM Asia Conference on Computer and Communications Security (ACM ASIACCS 2021)*, pp. 944-957, 7-11 June 2021, Hong Kong.
16. Haoran Yuan, Xiaofeng Chen, Guowen Xu, Jianting Ning, Joseph Liu, Robert H. Deng, “Efficient and verifiable proof of replication with fast fault localization”, *Proceedings of 2021 the IEEE International Conference on Computer Communications (INFOCOM 2021)*, pp. 1-10, 10-13 May 2021, Online.
17. Jiayun Xu, Yingjiu Li, and Robert H. Deng, “Differential training: a generic framework to reduce label noises for Android malware detection”, *Proceedings of the 2021 Network and Distributed System Security Symposium (NDSS 2021)*, 21-24 February 2021, Online.
18. Guowen Xu, Hongwei Li, Hao Ren, Jianfei Sun, Shengmin Xu, Jianting Ning, Haomiao Yang, Kan Yang, and Robert H. Deng, “Secure and verifiable inference in deep neural network”, *Proceedings of the 36th Annual Computer Security Applications Conference (ACSAC 2020)*, 7-11 December 2020, Online.
19. Guowen Xu, Hongwei Li, Yuan Zhang, Xiaodong Li, Robert H. Deng, Xuemin Shen, “A deep learning framework supporting model ownership protection and traitor tracing”, *Proceedings of the 26th IEEE International Conference on Parallel and Distributed Systems (ICPADS 2020)*, 2 – 3 December 2020, HK. **Best Paper**.
20. Jianting Ning, Xinyi Huang, Geong Sen Poh, Shengmin Xu, Jia-Ch’ng Loh, Jian Weng, Robert H. Deng, “Pine: enabling privacy-preserving deep packet inspection on TLS with rule-hiding and fast connection establishment”, *Proceedings of the 25th European Symposium on Research in Computer Security (ESORICS 2020)*, LNCS 12308, pp. 3-22, 14-18 Sept 2020, Guildford, UK. **Best Paper**.

21. Yang Liu, Zhuo Ma, Ximeng Liu, Siqi Ma, Surya Nepal, Robert. H. Deng, Kui Ren, “Boosting privately: federated extreme gradient boosting for mobile crowdsensing”, *Proceeding of the 40th IEEE International Conference on Distributed Computing Systems (ICDCS 2020)*, July 8 - 10, 2020, Singapore.
22. Xiangyu Wang, Jianfeng Ma, Ximeng Liu, Robert Deng, Yinbin Miao, Dan Zhu, Zhuoran Ma, “Search me in the dark: privacy-preserving Boolean range query over encrypted spatial data”, *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM 2020)*, pp. 2253-2262, 6-9 July 2020, Toronto, Canada
23. Guowen Xu, Hongwei Li, Shengmin Xu, Hao Ren, Yinghui Zhang, Jianfei Sun, Robert H. Deng, “Catch you if you deceive me: verifiable and privacy-aware truth discovery in crowdsensing systems”, *Proceedings of the 15th ACM Asia Conference on Computer and Communications Security (AsiaCCS 2020)*, pp. 178-192, 5-9 October 2020, Taiwan.
24. En He, Daoyuan Wu, Robert H. Deng, “Understanding Android VoIP security: a system-level vulnerability assessment”, *Proceedings of the 17th Conference on Detection of Intrusions and Malware & Vulnerabilities Assessment (DIMVA 2020)*, pp. 110-131, 24-26 June 2020, Lisboa, Portugal.
25. Siqi Ma, Runhan Feng, Juanru Li, Yang Liu, Surya Nepal, Elisa Bertino, Robert H Deng, Zhuo Ma, Sanjay Jha, “An empirical study of SMS one-time password authentication in Android apps”, *Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC 2019)*, pp. 339-354, 9-13 December 2019, San Juan, Puerto Rico.
26. Siqi Ma, Elisa Bertino, Surya Nepal, Juanru Li, Diethelm, Robert H. Deng and Sanjay Jha, “Finding flaws from password authentication code in Android Apps”, *Proceedings of the European Symposium on Research in Computer Security (ESORICS 2019)*, pp. 619-637 September, Luxembourg.
27. Pengfei Wu, Qingni Shen, Robert H. Deng, Ximeng Liu, Yinghui Zhang, and Zhonghai Wu, “OblIDC: an SGX-based oblivious distributed computing framework with formal proof”, *Proceedings of the ACM Asia Conference on Information, Computer and Communications Security (ASIACCS 2019)*, pp. 86-99, Auckland, New Zealand, July 7-12, 2019.
28. Yan Li, Zilong Wang, Yingjiu Li, Robert H. Deng, Binbin Chen, Weizhi Meng, Hui Li, “A Closer Look Tells More: A Facial Distortion Based Liveness Detection for Face Authentication (short paper)”, *Proceedings of the ACM Asia Conference on Information, Computer and Communications Security (ASIACCS 2019)*, short paper, pp. 241-246, Auckland, New Zealand, July 7-12, 2019.
29. Daoyuan Wu, Debin Gao, Eric KT Cheng, Yichen Cao, Jintao Jiang, Robert H. Deng, “Towards understanding Android system vulnerabilities: techniques and insights” *Proceedings of the ACM Asia Conference on Information, Computer and Communications Security (ASIACCS 2019)*, pp. 295-306, Auckland, New Zealand, July 7-12, 2019.
30. Ke Xu, Yingjiu Li, Robert H. Deng, Kai Chen, Jiayun Xu, “DroidEvolver: self-evolving Android malware detection system”, *Proceedings of the 4th IEEE European Symposium on Security and Privacy (EuroS&P 2019)*, pp. 47-62, Stockholm, Sweden, June 17-19, 2019.
31. Daoyuan Wu, Debin Gao, Rocky Chang, En He, Eric Cheng, and Robert H. Deng, “Understanding open ports in Android applications: discovery, diagnosis, and security assessment”, *Proceedings of the 26th Annual Network & Distributed System Security Symposium (NDSS 2019)*, 24-27 February 2019, San Diego, USA.

32. Ximing Liu, Yingjiu Li and Robert H. Deng, "Typing-Proof: usable, secure and low-cost two-factor authentication based on keystroke timings", *Proceedings of 2018 Annual Computer Security Applications Conference (ACSAC 2018)*, pp. 53-65, 3-7 Dec. 2018, San Juan, Puerto Rico, US.
33. Ximeng Liu, Kim-Kwang Raymond Choo, Robert H. Deng, Yang Yang, Yinghui Zhang, "PUSC: privacy-preserving user-centric skyline computation over multiple encrypted domains", *Proceedings of the 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (TrustCom 2018)*, pp. 958-963, 1-3 Aug. 2018, New York, NY, USA.
34. Ke Xu, Yingjiu Li, Robert H. Deng, and Kai Chen, "DeepRefiner: multi-layer Android malware detection system applying deep neural networks", *Proceedings of the 3rd IEEE European Symposium on Security and Privacy (EuroS&P 2018)*, pp. 473-487, 24-26 April 2018, London, UK.
35. Daoyuan Wu, Yao Cheng, Debin Gao, Yingjiu Li, Robert H. Deng, "SCLib: A Practical and Lightweight Defense against Component Hijacking in Android Applications", *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy (CODASPY 2018)*, pp. 299-306, 19-21 March 2018, Tempe, AZ, US.
36. Hui Cui, Man Ho Au, Baodong Qin, Robert H. Deng, Xun Yi, "Fuzzy public-key encryption based on biometric data", *Proceedings of the 11th International Conference on Provable Security (ProvSec 2017)*, LNCS 10592, 400-409, Springer, 23-25 October 2017, Xi'an, China.
37. Siqi Ma, Ferdian Thung, David Lo, Cong Sun and Robert H. Deng, "VuRLE: Automatic vulnerability detection and repair by learning from examples", *Proceedings of the 22nd European Symposium on Research in Computer Security (ESORICS 2017)*, LNCS 10493, pp. 229-246, Springer, 11-15 September 2017, Oslo, Norway.
38. Hui Cui, Robert H. Deng, Joseph K. Liu, and Yingjiu Li, "Attribute-Based Encryption with Expressive and Authorized Keyword Search", *Proceedings of the 22nd Australasian Conference on Information Security and Privacy (ACISP 2017)* LNCS 10342, Springer, pp. 106-126, 3-5 July 2017, Auckland, New Zealand.
39. Yan Li, Yao Cheng, Yingjiu Li, and Robert H. Deng, "What you see is not what you get: leakage-resilient password entry schemes for smart glasses", *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security (AsiaCCS 2017)*, pp. 327-333, April 2017, Abu Dhabi, UAE.
40. Hui Cui, Robert H. Deng, Guowei Wu and Junzuo Lai, "An efficient and expressive ciphertext-policy attribute-based-encryption scheme with partially hidden access structures", *Proceedings of the 10th International Conference on Provable Security (ProvSec 2016)*, LNCS 10005, pp. 19-38, 10-12 November 2016, Nanjing, China.
41. Dong Shen, Zhangkai Zhang, Xuhua Ding, Zhoujun Li and Robert H. Deng, "H-Binder: a hardened binder framework on Android systems", *Proceedings of the 12th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2016)*, pp. 24-43, 10-12 October 2016, Guangzhou, China.
42. Hui Cui, Robert H. Deng, Xuhua Ding and Yingjiu Li, "Attribute-based encryption with granular revocation", *12th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2016)*, 10-12 October 2016, Guangzhou, China.
43. Hui Cui, Robert H. Deng, Yingjiu Li, Baodong Qin, "Server-aided revocable attribute-based

- encryption”, *Proceedings of the 21st European Symposium on Research in Computer Security (ESORICS 2016)*, LNCS 9879, pp. 570-587, Heraklion, Greece, 26-30 September 2016.
44. Kai He, Jian Weng, Man Ho Au, Yijun Mao, and Robert H. Deng, “Generic anonymous identity-based broadcast encryption with chosen-ciphertext security”, *Proceedings of the 21st Australasian Conference on Information Security and Privacy (ACISP 2016)*, LNCS 9723, pp. 207-222, Springer, Melbourne, Australia, 4-6 July 2016.
 45. Yao Cheng, Yingjiu Li and Robert H. Deng, “A feasible no-root approach on Android”, *Proceedings of the 21st Australasian Conference on Information Security and Privacy (ACISP 2016)*, LNCS9723, pp. 481-489, Springer, Melbourne, Australia, 4-6 July 2016.
 46. Kai He, Jian Weng, Jia-Nan Liu, Joseph K. Liu, Wei Liu, and Robert H. Deng, “Anonymous identity-based broadcast encryption with chosen-ciphertext security”, *Proceedings of the 11th ACM Asia Conference on Computer and Communications Security (AsiaCCS 2016)*, pp. 247-255, Xi’an, China, 30 May – 3 June, 2016.
 47. Ngoc Hieu Tran, HweeHwa Pang, and Robert H. Deng, “Efficient verifiable computation of linear and quadratic functions over encrypted data”, *Proceedings of the 11th ACM Asia Conference on Computer and Communications Security (AsiaCCS 2016)*, pp. 605-616, Xi’an, China, 30 May – 3 June, 2016.
 48. Siqi Ma, David Lo, Teng Li, and Robert H. Deng, “CDRep: Automatic repair of cryptographic misuses in Android applications”, *Proceedings of the 11th ACM Asia Conference on Computer and Communications Security, (AsiaCCS 2016)*, pp. 711-722, Xi’an, China, 30 May – 3 June, 2016.
 49. Junzuo Lai, Robert H. Deng, Changshe Ma, Kouichi Sakurai and Jian Weng, “CCA-secure keyed-fully homomorphic encryption”, *Proceedings of the 19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC 2016)*, LNCS 9614, pp. 70-98, Tapei, Taiwan, March 6–9, 2016.
 50. Zhiguo Wan, Robert H. Deng and David Lee, “Electronic contract signing without using trusted third party”, *Proceedings of the 9th International Conference on Network and System Security (NSS 2015)*, LNCS 9408, pp. 386-394, New York, USA, 3-5 November 2015.
 51. Yan Li, Yingjiu Li, Qiang Yan, Hancong Kong and Robert H. Deng, “Seeing your face is not enough: an inertial sensor-based liveness detection for face authentication”, *Proceedings of the 22nd ACM Conference on Computer and Communications Security (CCS 2015)*, pp. 1558-1569, Denver, Colorado, USA, 12-16 October 2015.
 52. Zhuo Wei, Swee-Won Lo, Yu Liang, Tieyan Li, Jialie Shen, and Robert H. Deng, “Automatic accident detection and alarm system”, *Proceedings of ACM Multimedia Conference (MM 2015)*, pp. 781-784, Brisbane, Australia, 26-30 October 2015.
 53. Baodong Qin, Robert H. Deng, Yingjiu Li and Shengli Liu, “Server-aided revocable identity-based encryption”, *Proceedings of the 20th European Symposium on Research in Computer Security (ESORICS 2015)*, pp. 286-304, Vienna, Austria, 21-25 September 2015.
 54. Swee-Won Lo, Zhou Wei, Robert H. Deng and Xuhua Ding, “On security of content-based video stream authentication”, *Proceedings of the 20th European Symposium on Research in Computer Security (ESORICS 2015)*, pp. 366-383, Vienna, Austria, 21-25 September 2015.
 55. Daibin Wang, Haixia Yao, Yingjiu Li, Hai Jin, Deqing Zou and Robert H. Deng, “CICC: a fine-grained, semantic-aware, and transparent approach to preventing permission leaks for Android permission managers”, *Proceedings of the 8th ACM Conference on Security and*

- Privacy in Wireless and Mobile Networks (WiSec 2015)* pp. 6.1-6.6, New York City, 22-26 June, 2015,
56. Baodong Qin, Shenli Liu, Tsz Hon Yuen, Robert H. Deng, and Kefei Chen, “Continuous non-malleable key derivation and its application to related-key security”, *Proceedings of the 18th IACR International Conference on Practice and Theory in Public-Key Cryptography (PKC 2015)* pp. 557-578, Gaithersburg, MD, 30 May – 1 June, 2015.
 57. Yueqiang Cheng, Xuhua Ding, Robert H. Deng, “Efficient virtualization-based application protection against untrusted operating system”, *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2015)*, pp. 345-356, Singapore, April 14-17, 2015.
 58. Zhuo Wei, Robert H. Deng, Jialie Shen, Jixiang Zhu, Kai Ouyang, “Multidimensional context awareness in mobile devices”, *Proceedings of the 21st International Conference on Multimedia Modelling, (MMM 2015)*, pp. 38-49, 5-7 January 2015, Sydney, Australia.
 59. Swee-Won Lo, Zhuo Wei, Xuhua Ding and Robert H. Deng, “Generic attacks on content-based video stream authentication”, *Proceedings of 2014 IEEE International Conference on Multimedia and Expo (ICME 2014) Workshop*, 14-18 July 2014, Chengdu, China.
 60. Junzuo Lai, Robert H. Deng, Hweehwa Pang and Jian Weng, “Verifiable computation on outsourced encrypted data”, *Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS 2014)*, LNCS 8712, Springer, pp. 273-291, 7-11 September, 2014, Wroclaw, Poland.
 61. Jie Shi, Junzuo Lai, Yingjiu Li, Robert H. Deng and Jian Weng, “Authorized keyword search on encrypted data”, *Proceedings of the 19th European Symposium on Research in Computer Security (ESORICS 2014)*, LNCS 8712, Springer, pp. 419-435, 7-11 September, 2014, Wroclaw, Poland.
 62. Junzuo Lai, Robert H. Deng, Yingjiu Li and Weng Jian, “Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption”, *Proceedings of the 9th ACM SIGSAC Symposium on Information, Computer and Communications Security, (AsiaCCS 2014)*, pp. 239-248, 4-6 June 2014, Kyoto, Japan
 63. Yan Li, Ke Xu, Qiang Yan, Yingjiu Li and Robert H. Deng, “Understanding OSN-based facial disclosure against face authentication systems”, *Proceedings of the 9th ACM SIGSAC Symposium on Information, Computer and Communications Security (AsiaCCS 2014)*, pp. 413-424, 4-6 June 2014, Kyoto, Japan
 64. Junzuo Lai, Robert H. Deng, Shengli Liu, Jian Weng and Yunlei Zhao, “Identity-based encryption secure against selective opening chosen-ciphertext attack”, *Proceedings of Eurocrypt 2014*, LNCS 8441, Springer, pp. 77-92, 11-15 May 2014, Copenhagen, Denmark.
 65. Yueqiang Cheng, Zongwei Zhou, Miao Yu, Xuhua Ding and Robert H. Deng, “ROPecker: a generic and practical approach for defending against ROP attacks”, *Proceedings of the 21st Annual Network & Distributed System Security Symposium (NDSS 2014)*, 23-26 February 2014, San Diego, USA.
 66. Zhou Wei, Robert H. Deng, Jialie Shen, Yongdong Wu, Xuhua Ding and Swee Won Lo “Technique for authenticating H.264/SVC streams in surveillance applications”, *Proceedings of the 2013 IEEE International Conference on Multimedia and Expo (ICME 2013)*, Short Paper, San Jose, CA, 15-19 July 2013.
 67. Jin Han, Su Mon Kywe, Qiang Yan, Feng Bao, Robert H. Deng, Debin Gao, Yingjiu Li and Jianying Zhou, “Launching generic attacks on iOS with approved third-party applications”,

- Proceedings of the 11th International Conference on Applied Cryptography and Network Security (ACNS 2013), LNCS Vol. 7954, Springer, pp. 272-289, June 2013, Banff, Canada.
68. Yan Li, Yingjiu Li, Qiang Yan and Robert H. Deng, “Think twice before you share: analyzing privacy leakage under privacy control in online social networks”, *Proceedings of the 7th International Conference on Network and System Security (NSS 2013)* LNCS 7873, Springer, pp. 671-677, Madrid, Spain, June 2013.
 69. Junzuo Lai, Xuhua Zhou, Robert H. Deng, Yingjiu Li and Kefei Chen, “Expressive search on encrypted data”, *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (AsiaCCS 2013)*, pp. 243-252, 8-10 May 2013, Hangzhou, China
 70. Qiang Yan, Jin Han, Yingjiu Li, Jianying Zhou and Robert H. Deng, “Designing leakage-resilient password entry on touchscreen mobile devices”, *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security (AsiaCCS 2013)*, pp. 37-48, 8-10 May 2013, Hangzhou, China
 71. Junzuo Lai, Robert H. Deng, Yunlei Zhao and Jian Weng, “Accountable authority identity-based encryption with public traceability”, *Proceedings of the CT-RSA*, LNCS 7779, pp. 326-342, 25 February – 1 March 2013, San Francisco, USA.
 72. Jin Han, Qiang Yan, Debin Gao, Jianying Zhou and Robert H. Deng, “Comparing mobile privacy protection through cross-platform applications”, *Proceedings of the 20th Annual Network & Distributed System Security Symposium (NDSS 2013)*, 24-27 February 2013, San Diego, USA.
 73. Zhuo Wei, Xuhua Ding, Robert H. Deng and Yongdong Wu, “No tradeoff between confidentiality and performance: an analysis on H.264/SVC partial encryption”, *Proceedings of the 13th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2012)*, Springer, LNCS 7394, pp. 72-86, 3-5 September, 2012, Canterbury, UK. **Best Paper Award.**
 74. Yongdong Wu and Robert H. Deng, “A pollution attack to public-key watermarking schemes”, *Proceedings of the 2012 IEEE International Conference on Multimedia and Expo (ICME 2012)*, pp. 230-235, 9-13 July 2012, Melbourne, Australia.
 75. Shaoying Cai, Robert H. Deng, Yingjiu Li and Yunlei Zhao, “A new framework for privacy of RFID path authentication,” *Proceedings of the 10th International Conference on Applied Cryptography and Network Security (ACNS 2012)*, Springer, LNCS 7341, pp. 473-488, 26-29 June 2012, Singapore.
 76. Junzuo Lai, Robert H. Deng and Yingjiu Li, “Expressive CP-ABE with partially hidden access structures”, *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2012)*, 1-3 May 2012, Seoul, South Korea.
 77. Jie Shi, Darren Sim, Yingjiu Li and Robert H. Deng, “SecDS : a secure EPC discovery services system in EPCglobal network”, *Proceedings of the 2nd ACM Conference on Data and Application Security & Privacy (CODASPY 2012)*, pp. 267-274, 7-9 February 2012, San Antonio, Texas, USA.
 78. Qiang Yan, Jin Han, Yingjiu Li and Robert H. Deng, “On limitations of designing leakage-resilient password systems: attacks, principles and usability”, *Proceedings of the 19th Network and Distributed System Security Symposium (NDSS 2012)*, 5-8 February 2012, San Diego, California, USA. **Distinguished Paper Award.**
 79. Yongdong Wu and Robert H. Deng, “Zero-error watermarking on JPEG images by shuffling

- Huffman tree nodes”, *Proceedings of the Visual Communications and Image Processing (VCIP 2011)*, 6-9 November 2011, Tainan, Taiwan.
80. Yueqiang Cheng, Xuhua Ding and Robert H. Deng, “DriverGuard: a fine-grained protection on I/O flow”, *Proceedings of the European Symposium on Research in Computer Security (ESORICS 2011)* LNCS 6879, Springer, pp. 227-244, 12-14 September 2011, Leuven, Belgium.
 81. Jin Han, Qiang Yan, Robert H. Deng and Debin Gao, “On detection of erratic arguments”, *Proceedings of the 7th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2011)*, pp. 7-9 September 2011, London, UK.
 82. Feng Bao, Robert H. Deng, Xuhua Ding, Junzuo Lai and Yunlei Zhao, “Hierarchical identity-based chameleon hash and its applications”, *Proceedings of the 9th International Conference on Applied Cryptography and Network Security (ACNS 2011)*, LNCS 6715, Springer, pp. 201-219, 7-10 June 2011, Nerja, Spain.
 83. Qiang Yan, Jin Han, Yingjiu Li, Robert H. Deng and Tieyan Li, “A software-based root-of-trust primitive on multicore platforms”, *The 6th ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2011)*, pp. 334-343, 22-24 March 2011, Hong Kong.
 84. Cheng-Kang Chu, Wen Tao Zhu, Sherman Chow, Jianying Zhou and Robert H. Deng, “Secure mobile subscription of sensor-encrypted data”, *The 6th ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2011)*, pp. 228-237, 22-24 March 2011, Hong Kong.
 85. Junzuo Lai, Robert H. Deng and Shengli Liu, “Chameleon all-but-one TDFs and their application to chosen-ciphertext security”, *The 14th International Conference on Practice and Theory in Public Key Cryptography (PKC 2011)*, LNCS 6571, Springer, pp. 228-245, 6-9 March 2011, Taormina, Italy.
 86. Shaoying Cai, Chunhua Su, Yingjiu Li, Tieyan Li and Robert H. Deng, “Protecting and restraining the third party in RFID-enabled 3PL supply chains”, *Proceedings of the Sixth International Conference on Information Systems Security (ICISS 2010)*, LNCS 6503, Springer, pp. 246-260, 15-19 December 2010, DA-IICT, Gandhinagar Gujarat, India.
 87. Robert H. Deng, Yingjiu Li, Moti Yung and Yunlei Zhao, “A new framework for RFID privacy”, *Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS 2010)*, LNCS 6345, Springer, pp. 1-18, 20-22 September 2010, Athens, Greece.
 88. Junzuo Lai, Robert H. Deng and Yingjiu Li, “Revisiting unpredictability-based RFID privacy models”, *Proceedings of the 8th International Conference on Applied Cryptography and Network Security (ACNS 2010)*, LNCS 6123, Springer, pp. 475-492, June 2010, Beijing, China.
 89. Sherman S. M. Chow, Jian Weng, Yanjiang Yang, Robert H. Deng, “Efficient Unidirectional Proxy Re-Encryption”, *Proceedings of the Third International Conference on Cryptology in Africa, (AFRICACRYPT 2010)*, LNCS 6055, Springer, pp. 316-332, May 2010, Stellenbosch, South Africa.
 90. Cheng-Kang Chu, Joseph K. Liu, Jianying Zhou, Feng Bao and Robert H. Deng, “Practical ID-based encryption for wireless sensor network”, *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2010)*, pp. 337-340, 13-16 April, 2010, Beijing, China.
 91. Junzuo Lai, Robert H. Deng, Shengli Liu and Weidong Kou, “Efficient CCA-secure public key encryption from identity-based techniques”, *Proceedings of the Cryptographers’ Track*

- at the *RSA Conference (CT-RSA 2010)*, LNCS 5985, Springer, pp. 132-147, 1-5 March 2010, San Francisco, CA, USA.
92. Liang Gu, Yueqiang Cheng, Xuhua Ding, Robert H. Deng, Yao Guo and Weizhong Shao, "Remote attestation on function execution", *Proceedings of the First International Conference on Trusted Systems (Intrust 2009)*, LNCS 6163, Springer, pp. 60-72, 17-19 December 2009, Beijing, China.
 93. Yanjiang Yang, Jianying Zhou, Robert H. Deng and Feng Bao, "Computationally secure hierarchical self-healing key distribution for heterogeneous wireless sensor networks", *Proceedings of the 11th International Conference on Information and Communications Security (ICICS 2009)*, LNCS 5927, Springer, pp. 135-149, acceptance rate = 18.9%, 14-17 December 2009, Beijing, China.
 94. Shaoying Cai, Tiejian Li, Changshe Ma, Yingjiu Li, and Robert H. Deng, "Enabling secure secret updating for unidirectional key distribution in RFID-enabled supply chains", *Proceedings of the 11th International Conference on Information and Communications Security (ICICS 2009)*, LNCS 5927, Springer, pp. 150-164, acceptance rate = 18.9%, 14-17 December 2009, Beijing, China.
 95. Changshe Ma, Yingjiu Li, Robert H. Deng and Tiejian Li, "RFID privacy: relation between two notions, minimal condition, and efficient construction", *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS 2009)*, pp. 54-65, 9-13 November 2009, Chicago, USA.
 96. Qi Zhang, Yi Mu, Minjie Zhang, and Robert H. Deng, "Secure mobile agents with designated hosts", *Proceedings of the 3rd International Conference on Network & System Security (NSS 2009)*, pp. 286-293, 19-21 October 2009, Gold Coast, Australia.
 97. Yanjiang Yang, Jianying Zhou, Robert H. Deng and Feng Bao, "Hierarchical self-healing key distribution for heterogeneous wireless sensor networks", *Proceedings of the 5th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2009)*, pp. 285-295, 14-18 September 2009, Athens, Greece.
 98. Jian Weng, Yanjiang Yang, Qiang Tang and Robert H. Deng, "Efficient conditional proxy re-encryption with chosen-ciphertext security", *Proceedings of the 2009 Information Security Conference (ISC 2009)*, LNCS 5735, Springer, pp. 151-166, 7-9 September, 2009, Pisa, Italy.
 99. Kar Way Tan and Robert H. Deng, "Applying sanitizable signature to web-service-enabled business processes: going beyond integrity protection", *Proceedings of the IEEE 7th International Conference on Web Services (ICWS 2009)*, pp. 67-74, 6-10 July, 2009, Los Angeles, USA.
 100. Jin Han, Debin Gao and Robert H. Deng, "On the effectiveness of software diversity: a systematic study on real-world vulnerabilities", *Proceedings of the 6th SIG SIDAR Conference on Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2009)*, LNCS 5587, Springer, pp. 127-146, 9-10 July, 2009, Milan, Italy.
 101. Cheng-Kang Chu, Jian Weng, Sherman Chow, Jianying Zhou and Robert H. Deng, "Conditional proxy broadcast re-encryption", *Proceedings of the 14th Australasian Conference on Information Security and Privacy (ACISP 2009)*, LNCS 5594, Springer, pp. 327-342, 1-3 July 2009, Brisbane, Australia.
 102. Shaoying Cai, Tiejian Li, Yingjiu Li and Robert H. Deng, "Ensuring dual security modes in RFID-enabled supply chain systems", *Proceedings of the 5th Information Security Practice and Experience Conference (ISPEC 2009)*, LNCS 5451, pp. 372-383, Springer, 13-15 April

2009, Xi'an, China.

103. Shaoying Cai, Yingjiu Li, Tiejian Li and Robert H. Deng, "Attacks and improvements to an RFID mutual authentication protocol", *Proceedings of the 2nd ACM Conference on Wireless Network Security (WiSec 2009)*, pp. 51-58, 16th-19th March, 2009, Zurich, Switzerland.
104. Jian Weng, Robert H. Deng, Cheng-kang Chu, Xuhua Ding and Junzuo Lai, "Conditional Proxy Re-Encryption Secure against Chosen-Ciphertext Attack", *Proceedings of the 2009 ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2009)*, pp. 54-65, 10-12 March 2009, Sydney, Australia.
105. Robert H. Deng, Jian Weng, Shengli Liu and Kefei Chen, "Chosen-ciphertext secure proxy re-encryption without pairing", *Proceedings of the 7th International Conference on Cryptology and Network Security (CANS 2008)*, LNCS 5339, pp. 1-17, Springer, December 2-4, 2008, Hong Kong, China.
106. Liang Gu, Xuhua Ding, Robert H. Deng, Bing Xie and Hong Mei, "Remote attestation on program execution", *Proceedings of the Third ACM Workshop on Scalable Trusted Computing (STC 2008)*, pp. 11-19, 31st October 2008, Fairfax, VA, USA.
107. Yanjiang Yang, Xuhua Ding, Robert H. Deng and Feng Bao, "An efficient PIR construction using trusted hardware", *Proceedings of the 11th Information Security Conference (ISC 2008)*, LNCS 5222, pp. 64-79, Springer, September 15-18, 2008, Taipei, Taiwan.
108. Hyundo Park, Peng Li, Debin Gao, Heejo Lee and Robert H. Deng, "Distinguishing between FE and DDoS using randomness check", *Proceedings of the 11th Information Security Conference (ISC 2008)*, LNCS 5222, pp. 131-145, Springer, September 15-18, 2008, Taipei, Taiwan.
109. Feng Bao, Robert H. Deng, Xuhua. Ding and Yanjiang. Yang, "Private query on encrypted data in multi-user settings", *Proceedings of the 4th Information Security Practice and Experience Conference (ISPEC 2008)*, LNCS 4991, pp. 71-85, Springer, April 21-23, Sydney, Australia.
110. Y. Wu, F. Bao and R. H. Deng, "Forgery attack to an asymptotically optimal traitor tracing scheme", *Proceedings of the 12th Australasian Conference on Information Security and Privacy (ACISP 2007)*, LNCS 4586, pp. 171-183, Springer, July 2nd-4th, 2007, Queensland, Australia.
111. Y. Yang, R. H. Deng and F. Bao, "Practical private data matching deterrent to spoofing attacks", *Proceedings of ACM 15th Conference on Information and Knowledge Management (CIKM)*, pp. 852-853, Arlington, VA, USA, Nov. 2006.
112. D. J. T. Chong and R. H. Deng, "Privacy-enhanced superdistribution of layered content with trusted access control", *Proceedings of the 6th ACM Workshop on Digital Rights Management (DRM 2006)*, pp. 37-44, October 30, 2006, Alexandria VA, USA.
113. S. Wang, X. Ding, R. H. Deng, and F. Bao, "Private information retrieval using trusted hardware", *Proceedings of the 11th European Symposium on Research in Computer Security (ESORICS 2006)*, LNCS 4189, pp. 49-64, Springer, September 18-20, 2006, Hamburg, Germany
114. J. Guo, Y. Li, R. H. Deng and K. Chen, "Rights protection for data cubes", *Proceedings of the 9th International Conference (ISC 2006)*, LNCS 4176, pp. 359-372, Springer, August 30 – September 2, 2006, Samos Island, Greece.
115. Y. Li, H. Liu and R. H. Deng, "Practical inference control for data cubes", *Proceedings of the IEEE Symposium on Security and Privacy (S&P 2006)*, pp. 115-120, May 2006, Oakland, CA,

USA.

116. Y. Li and R. H. Deng, "Publicly verifiable ownership protection for relational databases", *Proceedings of the ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2006)* Taipei, Taiwan, March 2006.
117. Y. Yang, R. H. Deng and F. Bao, "Fortifying password authentication in integrated healthcare delivery systems", *Proceedings of the ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2006)* Taipei, Taiwan, March 2006.
118. Z. Wan, R. H. Deng, F. Bao and A. L. Ananda, "Anonymous DoS-Resistant Access Control Protocol Using Passwords for Wireless Networks", *Proceedings of IEEE Conference on Local Computer Networks (LCN 2005)*, pp. 328-335, Sydney, Australia, 15-17 November 2005.
119. Y. Yang, F. Bao and R. H. Deng, "Security analysis and fix of an anonymous credential system", The 10th Australasian Conference on Information Security and Privacy (**ACISP 2005**), LNCS 3574, Springer, pp. 537-547, Brisbane, Australia, July 2005
120. Y. Wu, H. Pang and R. H. Deng, "How much you watch, how much you pay", *Proceedings of SPIE Visual Communications and Image Processing (VCIP 2005)* 2005, SPIE Vol. 5960, pp.961-968, July 12-15, 2005, Beijing, China
121. Y. Wu, F. Bao and R. H. Deng, "Secure human communications based on biometrics signals", *The 20th IFIP International Information Security Conference (ISC 2005)* May 30 - June 1, 2005, Makuhari-Messe, Chiba, Japan.
122. Y. Wu, T. Li and R. H. Deng, "Protecting group dynamic information in large scale multicast groups", *The 20th IFIP International Information Security Conference (ISC 2005)* May 30 - June 1, 2005, Makuhari-Messe, Chiba, Japan.
123. Y. Yang, E. Bertino, B. C. Ooi and R. H. Deng, "Privacy and ownership preserving of outsourced medical data", *Proceedings of the IEEE 21st International Conference on Data Engineering (ICDE 2005)* 5th - 8th April 2005, Tokyo, Japan.
124. B. Zhu, Z. Wan, M. Kankanhalli, F. Bao and R. H. Deng, "Anonymous secure routing in mobile ad-hoc networks", *The 29th Annual IEEE Conference on Local Computer Networks (LCN 2004)*, 16th-18th November, 2004, Tampa, Florida, USA.
125. Y. Wu, D. Ma and R. H. Deng, "Progressive protection of JPEG2000 code-streams", *Proceedings of the IEEE International Conference on Image Processing (ICIP 2004)* pp. 3439-3442, 24-27 October 2004, Singapore.
126. Y. Wu and R. H. Deng, "Compliant encryption of JPEG2000 codestreams", *Proceedings of the IEEE International Conference on Image Processing (ICIP 2004)* pp. 3447-3450, 24-27 October 2004, Singapore.
127. G. Wang, R. H. Deng, D. Kwak, and S. Moon. "Security Analysis of Two Signcryption Schemes". *Information Security Conference (ISC 2004)*, LNCS 3225, pp. 123-133, September 27-29, 2004, Palo Alto, CA, USA.
128. B.-M. Goi, R. C. Phan, Y. Yang, F. Bao, R. H. Deng and M. U. Siddiqi, "Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity", *Applied Cryptography and Network Security (ACNS 2004)*, LNCS 3089, pp. 369-382, China, June 8-11, 2004.
129. C. Peng, R. H. Deng, Y. Wu and W. Shao, "A flexible and scalable authentication scheme for JPEG2000 image codestreams", *Proceedings of the 11th ACM International Conference on Multimedia (MM 2003)* pp. 433-441, 4th-6th November 2003, Berkeley, USA.

130. J. Zhou, F. Bao and R. H. Deng, "Validating digital signatures without TTP's time-stamping and certificate revocation", *6th Information Security Conference (ISC 2003) Lecture Notes in Computer Science 2851*, pp. 96-110, 1st-3rd October 2003, Bristol, UK.
131. F. Bao, R. H. Deng and H. Zhu, "Variations of Diffie-Hellman problem", *5th International Conference on Information and Communications Security (ICICS 2003) Lecture Notes in Computer Science 2836*, Springer , pp. 301-312, 9th-13th October 2003, China.
132. Y. Yang, F. Bao and R. H. Deng, "Flexible authentication of images", *Visual Communications and Image Processing 2003 (VCIP 2003)* pp. 1905-1911, 8th-11th July 2003, Lugano, Switzerland.
133. R. H. Deng, J. Zhou and F. Bao, "Defending against redirect attacks in mobile IP", *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS 2002)* pp. 59-67, November 2002, Washington DC.
134. F. Bao and R. H. Deng, "Privacy protection for transactions of digital goods", *Proceedings of the Third International Conference on Information and Communications Security (ICICS 2001), Lecture Notes in Computer Science 2229*, Springer, pp. 202-213, 13th-16th November 2001, Xian, China.
135. H. Wu, F. Bao, R. H. Deng, "Cryptanalysis of a digital signature scheme on ID-based key-sharing infrastructure," *Proceedings of the 2001 International Workshop on Practice and Theory in Public Key Cryptography (PKC 2001) Lecture Notes in Computer Science 1992*, pp. 173-179, 13th-15th February 2001, Cheju Island, Korea.
136. F. Bao, R. H. Deng, W. Geiselmann, C. Schnorr, R. Steinwandt, H. Wu, "Cryptanalysis of two sparse polynomial based public key cryptosystems", *Proceedings of the 2001 International Workshop on Practice and Theory in Public Key Cryptography (PKC 2001) Lecture Notes in Computer Science 1992*, pp.153-164, 13th-15th February 2001, Cheju Island, Korea.
137. H. Wu, F. Bao, D. Ye, R. H. Deng, "Cryptanalysis of polynomial authentication and signature scheme", *Proceedings of the 5th Australasian Conference on Information Security and Privacy (ACISP 2000), Lecture Notes in Computer Science 1841*, pp. 278-288, Springer Verlag, July 2000, Australia.
138. H. Wu, F. Bao, D. Ye, R. H. Deng, "Cryptanalysis of the m-permutation protection schemes", *Proceedings of the 5th Australasian Conference on Information Security and Privacy (ACISP 2000) Lecture Notes in Computer Science 1841*, pp. 97-111, Springer Verlag, July 2000, Australia.
139. J. Zhou, R. H. Deng, and F. Bao, "Some remarks on fair exchange protocol", *Proceedings of 2000 International Workshop on Practice and Theory in Public Key Cryptography (PKC 2000) Lecture Notes in Computer Science 1751*, pp. 46-57, January 2000, Melbourne, Australia.
140. J. Zhou, R. H. Deng, and F. Bao, "Evaluation of fair non-repudiation with TTP", *Proceedings of the 4th Australasian Conference on Information Security and Privacy (ACISP 1999) Lecture Notes in Computer Science 1587*, pp. 258-269, Springer-Verlag, July 1999, Australia.
141. F. Bao and R. H. Deng, "A new type of "magic ink" signatures – towards transcript-irrelevant anonymity revocation", *Proceedings of the International Workshop on Practice and Theory in Public Key Cryptography (PKC 1999) Lecture Notes in Computer Science 1560*, pp. 1-11, March 1999, Kamakura, Japan.

142. H. Wu, F. Bao, R. H. Deng and Z. Ye, "Cryptanalysis on Rijmen-Preneel trapdoor ciphers", *Advances in Cryptology (Asiacrypt 1998)*, *Lecture Notes in Computer Science 1514*, Springer-Verlag, 1998, pp.126-132, October 1998, Beijing, China
143. H. Wu, F. Bao, R. H. Deng and Z. Ye, "Improved truncated differential attack on SAFER", *Advances in Cryptology (Asiacrypt 1998)*, *Lecture Notes in Computer Science 1514*, Springer-Verlag, pp. 133-147, October 1998, Beijing, China.
144. F. Bao, R. Deng, and W. Mao, "Efficient and practical fair exchange protocols", *1998 IEEE Symposium on Security and Privacy (S&P 1998)*, pp. 77-85, May 1998, Oakland, CA.
145. F. Bao and R. Deng, "A signcrytion scheme with signature verification not using recipient's private key", *Proceedings of the International Workshop on Practice and Theory in Public Key Cryptography (PKC 1998)*, Springer-Verlag, *Lecture Notes in Computer Science 1431*, pp. 55-59, January 1998, Yokohama, Japan.
146. F. Bao, R. H. Deng, Y. Han, and A. Jeng, "Design and analysis of two basic protocols for use in TTP-based key escrow schemes," *Proceedings of 1997 the Australasian Conference on Information Security and Privacy (ACISP 1997)*, *Lecture Notes in Computer Science 1270*, Springer-Verlag, pp. 261-270, 7th-9th July 1997, Sydney, Australia.
147. R. H. Deng, Y. Han, A. B. Jeng, and T.-H. Ngair, "A new on-line cash check scheme", *Proceedings of the 4th ACM Conference on Computer and Communications Security (CCS 1997)* pp. 111-116, Zurich, Switzerland, April 1997.
148. F. Bao, R. H. Deng, Y. Han, A. Jeng, D. Narasimhalu, and T. Ngair, "Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults", In B. Christianson, B. Crispo, M. Lomas, and M. Roe Editors, **Security Protocols**, *Lecture Notes in Computer Science 1361*, pp. 115-124, 1997.
149. R. H. Deng, L. Gong, A. A. Lazar, W. Wang, "Authenticated key distribution and secure broadcast using no conventional encryption: a unified approach based on block codes," *Proceedings of IEEE Globecom 1995*, pp. 1193-1197, November 1995, Singapore.
150. R. H. Deng, L. Gong, A. A. Lazar, "Securing data transfer in asynchronous transfer mode networks," *Proceedings of IEEE Globecom 1995*, pp. 1198-1202, November 1995, Singapore.
151. R. H. Deng, S. K. Bhonsle, W. Wang, and A. A. Lazar, "Integrating security in CORBA based object architectures," *Proceedings of the 1995 IEEE Symposium on Security and Privacy (S&P 1995)* pp. 50-61, May 1995, Oakland, CA.
152. R. H. Deng, W. C. L. Chiew, and K. T. Huang, "Analysis of token-ring networks with both finite and infinite buffer capacity stations," *Proceedings of IEEE INFOCOM 1991*, April 1991, pp. 202-210, Miami, Florida.
153. R. H. Deng, X. Y. Zhang and K. T. Huang, "Token-passing systems with batch arrivals and their application to multimedia file transfer over token-ring LANs," *Proceedings of IEEE INFOCOM 1991*, pp. 1041-1049, April 1991, Miami, Florida.
154. S. Pietrobon, D. J. Costello, Jr., G. Ungerboeck, R. H. Deng, and A. LaFanechere, "Channel coding with muti-dimensional trellis coded phase modulation," *Presented at 1988 International Symposium on Information Theory (ISIT 1988)*, June 1988, Kobe, Japan.
155. D. J. Costello, Jr. and R. H. Deng, "Multi-dimensional unit-memory and partial-unit-memory trellis coded modulation," *Presented at the 1987 Conference on Information Sciences and Systems*, March 1987, Baltimore, MD.

156. M. A. Herro and R. H. Deng, "Error-correcting DC-free binary transmission codes for fiber optic digital communications," *Proceedings of the 1987 Conference on Information Sciences and Systems*, pp. 559-564, March 1987, Baltimore, MD.
157. M. A. Herro, L. Z. Hu, D. J. Costello, Jr., and R. H. Deng, "Performance of convolutional codes on noisy channels," *Presented at the 1986 IEEE International Symposium on Information Theory (ISIT 1986)*, August 1986, Ann Arbor, MI.
158. D. J. Costello, Jr. and R. H. Deng, "Concatenated coding systems employing bandwidth efficient inner codes," *Presented at the 1986 IEEE International Symposium on Information Theory (ISIT 1986)*, August 1986, Ann Arbor, MI.
159. R. H. Deng and D. J. Costello, Jr., "Performance of a concatenated coding system," *Proceedings of the Twenty-Second Annual Allerton Conference on Communication, Control, and Computing*, pp. 535-544, October 1984, Allerton, IL.

Book Reviews, Editorials and Electronic Publications

1. Elisa Bertino, Robert H. Deng, Xinyi Huang, Jianying Zhou, "Editorial: Security and privacy of electronic health information systems", *International Journal of Information Security*, Vol. 14, No. 6, pp. 485-486, November 2015.
2. Zheng Yan, Guojun Wang, Valtteri Niemi, Robert H. Deng, "Editorial: Special issue on trust in cyber, physical and social computing", *Computers & Security*, pp. 1-2, November 2014.
3. Robert H. Deng, Zheng Yan, Audun Josang, Guojun Wang, "Editorial: Special issue on trust and identity management in mobile and Internet computing and communications", *IET Information Security*, Vol. 7, No. 1, pp. 1-2, March 2013.
4. Robert H. Deng, Jari Veijalainen, Shiguo Lian and Dimitris Kanellopoulos, "Editorial: special issue on ubiquitous electronic commerce systems", *Journal of Electronic Commerce Research*, Vol. 11, No. 1, pp. 1-4, January 2011.
5. F. Bao, R. H. Deng, Y. Han, A. Jeng, D. Narasimhalu, and T. Ngair, "New attacks to public key cryptosystems on tamperproof devices", *IEEE Electronic Cipher News Letters*, 29th Sept. 1996, <http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/news-items/>.
6. F. Bao, R. H. Deng, Y. Han, A. Jeng, D. Narasimhalu, and T. Ngair, "A method to counter another new attack to RSA on tamperproof devices", *IEEE Cipher News Letters*, 24th Sept. 1996, <http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/news-items961024.sgtampercounter.html>
7. F. Bao, R. H. Deng, Y. Han, A. Jeng, D. Narasimhalu, and T. Ngair, "Another new attack to RSA on tamperproof devices", 23rd Sept. 1996, *IEEE Electronic Cipher News Letters*, <http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/newsitems/961022.sgtamper.html>.
8. R. H. Deng, (invited book review) "Web security sourcebook: a complete guide to web security threats and solutions" *Journal of Computer Communications*, p. 591, Vol. 22, No. 6, April 1999.
9. R. H. Deng (invited book review), "Invaluable state-of-the-art reference," for *Journal of Computer Communications*, Vol. 18, No. 1, pp. 58-59, January 1995.
10. R. H. Deng (invited book review), "Bring network security out of the closet," *Journal of Computer Communications*, Vol. 18, No. 1, pp. 55-56, January 1995.
11. R. H. Deng (invited book review), "Comprehensive token ring coverage," *Journal of Computer Communications*, Vol. 17, No. 1, pp. 75-76, January 1994.

Contributions to International Standards

1. Y. Wu, R. H. Deng, D. Ma, C. Peng, and Y. Yang, "Authentication of JPEG 2000 code-streams and files", incorporated in ISO/IEC JPSEC 15444-8, April 2007.
2. Y. Wu, R. H. Deng, "A Method for JPEG 2000 Access Structure", incorporated in ISO/IEC JPSEC 15444-8, April 2007.

Patents Granted

1. Robert H. Deng, Yinghui Zhang, "Cloud data sharing systems and methods for sharing data using the systems", Singapore patent 10202007162Q, filed on 27 July 2020.
2. Ximing Liu, Robert H. Deng, Yingjiu Li, "Systems and methods for two-factor authentication", Singapore patent 10201801032U, 6 July 2021.
3. Hui Cui, R. H. Deng, Y. Li, G. Wang, and T. H. Yuen, "Data processing method and apparatus", US patent 10868670, 25 December 2020.
4. Yang Yang, Haiguang Wang, Xin Kang, Robert H. Deng, "Zero-touch IoT device deployment based on distributed ABE", China patent CN202011010134.3, 23 September 2020.
5. Hui Cui, Robert H. Deng, Yingjiu Li, Guilin Wang, and Tsz Hon Yuen, "Data processing method and apparatus", US patent US20190173668A1, 6 June 2019.
6. Ke Xu, Yingjiu Li, Robert H. Deng, "System and method for determining a security classification of an unknown application", US patent US20180096142, 5 April 2018.
7. Robert H. Deng and Yingjiu Li, "Data security system and method for operation thereof", Singapore patent 10201508390P, 9th October 2015; PCT WO2017061950 A1, 13 April 2017.
8. Ke Xu, Yingjiu Li and Robert H. Deng, "System and method for determining a security classification of an unknown application". Singapore patent 10201504543V, PCT/SG2016/050145, 15 December 2016.
9. Hui Cui, Zhiguo Wan, Robert H. Deng, and Guilin Wang, "Expressive searchable encryption", Singapore patent SG10201608619P, 14 October 2016.
10. Hui Cui, Robert H. Deng, Yingjiu Li, Guilin Wang, and Yuen Tsz Hon, "Data processing method and device", China patent CN201610640301.X, 5 August 2016; SG-0050328, 30 June 2017 and WO-0026323, 8 February 2018.
11. Zhou Wei and Robert H. Deng, "Method and system for correcting eye gaze direction in an image", Singapore Patent 10201503664P, 11th May 2015.
12. Zhuo Wei, Robert H. Deng and Chengfang Fang, "Method and system for accident avoidance", Singapore Patent 10201406053Q, 25th September 2014; PCT/SG2015/050329, 31 March 2016.
13. Y. Wu and R. H. Deng, "Method for incremental authentication of documents", US 7,315,866, 1st January 2008.
14. F. Bao, J. Zhou and R. H. Deng, "Method of generating an authentication", SG 110390, 28th February 2007. US 7,233,782, 19 June 2007.
15. R. H. Deng, F. Bao, T. Li, A. Lakshminarayanan, a "Method for cryptographically processing a message, method for generating a cryptographically processed message, method for performing a cryptographic operation on a message, computer system, client computer, server computer and computer program elements", SG120791; US patent US20060285683 A1, 1 Oct 2004.

16. D. Ye, F. Bao, R. H. Deng and H. Wu, "Method and apparatus for constructing efficient elliptic curve cryptosystems", SG 99167, 27th January 2006; US Patent 20040158597 A1.
17. Y. Wu, R. H. Deng, F. Bao, "Remote authentication based on exchanging signals representing biometrics information", SG 95612, 30th November 2004; US 6910129, 21st June 2005.
18. J. Wu, Q. Sun and R. H. Deng, "Legitimacy protection of electronic document and a printed copy thereof", GB 2365184, 16th June 2004.
19. R. H. Deng, P. Feng and F. Bao, "Private retrieval of digital objects", SG 103257, 29th April 2004; US 7,231,047, 12th June 2007.
20. P. Feng, F. Bao and R. H. Deng, "Method and apparatus for providing XML document encryption", US 2004/0078577A1, 22nd April 2004; Singapore Patent No. 97038, 31st October 2005.
21. J. Zhou, F. Bao and R. H. Deng, "A public key cryptography and a framework therefore", Singapore 110701, 30th April 2007.
22. R. H. Deng and Y. Wu, "Method and apparatus for digital content copy protection", SG 97852, US 6711553, 23rd March 2004.
23. F. Bao, R. H. Deng, and H. Wu, "A method of sale auditing in private transaction of e-goods", PCT WO 03/044619 A2, 30th May 2003; SG 104005, 31st May 2006
24. Q. Sun, J. Wu and R. H. Deng, "Method and apparatus for embedding digital information in digital multimedia data", US 6,678,389, 13 Jan 2004; SG 81505, 30th July 2004; GB 2,366,112, 28th May 2003.
25. Q. Sun, J. Wu, R. H. Deng, "Method and apparatus for protecting the legitimacy of an article", GB 2,364,513, 9th April 2003; US 6,748,533, 8th June 2004, SG81478, 28th November 2003.
26. J. Hu, F. Bao, R. H. Deng, "A method of data storage and apparatus therefor", GB 2,349,964, 24th July 2002; SG 73941, 30th Sept 2002.
27. F. Bao and R. H. Deng, "A method of exchanging digital data", SG 75691, 20th Sept 2002; European patent 1082836, 23 November 2005; US 7,171,559, 30th January 2007.
28. B. Feng, R. H. Deng, "Method and apparatus for encrypting and decrypting data", SG 82916, 23rd May 2002; US 7,110,539, 19th September 2006.
29. R. H. Deng and T. Ngair, "Microprocessor card payment system", SG 67957, 19th April 2002.
30. R. H. Deng and Y. Wu, "Method and apparatus for digital content copy protection", US 6,711,553, 23rd March 2004, SG97852, 29th October 2004.
31. N. A. Desai, R. H. Deng, and W. Wang, "Computationally efficient method for trusted and dynamic digital objects dissemination", SG 67354, 18th July 2000; US 6058383, 2nd May 2000.
32. R. H. Deng, Y. X. Li, and E. H. Koh, "Correcting up to two disc drive read errors and detecting the occurrence of more than two read errors ", US 5627843, 6th May 1997.

7 Notable Research Grants and Projects

1. Towards zero-trust collaborative computing ecosystem (Jan 2024 – Dec 2026): co-Principal Investigator. Project funding of \$5,199,870.00 from Singapore Cybersecurity Agency; Principal Investigator of subproject 3 at \$1,23,7000.00.
2. Trusted decentralized identities (May 2024 – April 2027): co-Principal Investigator. Project funding of \$1,613,872.00 from Digital Trust Centre.
3. Attribute-based authentication and authorization technologies (July 2021- July 2023): Principal Investigator. Project funding of S\$608,000.00 from Huawei International Pte Ltd.

4. sBox – secure enterprise cloud data storage system (Sept 2020 – Mar 2022): Principal Investigator. Project funding of \$250,000.00 from SMART Innovation Centre.
5. Zero touch identity management for IoT devices (August 2019- July 2020): Principal Investigator. Project funding of S\$274,300.00 from Huawei International Pte Ltd.
6. National Satellite of Excellence in Mobile Systems Security and Cloud Security (April 2019 – March 2024): Programme Director. Project funding of S\$7,564,320.00 under Singapore’s National Cybersecurity Research and Development Program.
7. Automatic labeling of malicious behavior using machine learning (October 2018 – October 2019): co-Principal Investigator, Project funding of S\$279,500.00 from Huawei International Pte Ltd.
8. Intelligent and non-intrusive monitoring of Android devices for protection against data-infringing malware (July 2018 – Dec 2020). co-Principal Investigator, Project funding of \$206,736.00 from AI Singapore.
9. Building next-generation secure environments on smartphones for critical mobile applications (Award #: NRF2016NCR-NCR002-022, October 2017 – Sept 2019): Principal Investigator. Project funding of S\$879,886.08 under Singapore’s National Cybersecurity Research and Development Program.
10. COMMANDO-HUMANS - COMputational Modelling and Automatic Non-intrusive Detection Of HUMAN behAviour based iNSecurity (Award #: NRF2015NCR-NCR003-002, April 2016 – May 2018): Lead Principal Investigator. Project funding of S\$416,021 under Singapore’s National Cybersecurity Research and Development Program.
11. Secure Mobile Centre – Technologies and Solutions for Securing Mobile Computing (Award #: NRF2014NCR-NCR001-012, February 2015- February 2019): Lead Principal Investigator. Project funding of S\$6,415,200 under Singapore’s National Cybersecurity Research and Development Program.
12. Advanced Defense Techniques for Mobile Systems and Future Networks (June 2015- June 2016): Lead Principal Investigator. Project funding of S\$729,196 from Huawei Technologies Co. Ltd.
13. Multidimensional context awareness security techniques (December 2013- December 2014): Principal Investigator. Project funding of S\$156,000.00 from Huawei Technologies Co. Ltd.
14. Techniques and Systems for Securing Scalable Multimedia Content Dissemination (SERC Grant #: 1021010027, August 2010-July 2013): Principal Investigator. Project funding of S\$504,480 under A*STAR SERC Public Sector R&D Funding Scheme. The Use of Mobile Devices in RFID-based Supply Chain Management (September 2009- September 2010): Principal Investigator. Project funding of S\$20,108 from Nokia Research Center, Beijing, China.
15. Security Framework for EPCglobal Network (SERC Grant #: 082 1010022, August 2008-July 2011): Co-Principal Investigator. Project funding of S\$479,700 under A*STAR SERC Public Sector R&D Funding Scheme.
16. Security Architecture and Techniques for Communications, Control and Management of Energy Distribution Systems (SERC Grant #: 0721330047, March 2008-February 2011). Co-Principal Investigator. Project funding of S\$470,425 under A*STAR SERC Intelligent Energy Distribution Systems (IEDS) Thematic Research Grant.
17. TeleOph – A Secure Tele-ophthalmology System (TEC Reference No. P00619/1332, August 2007- August 2008): University Project Manager. Project funding of S\$329,600 by TEC (The Enterprise Challenge Program in the Prime Minister’s Office).

8 Keynotes, Invited Talks and Panel Discussions

1. Keynote, “Privacy preserving service discovery in wireless communications”, *The 4th International Conference on Ubiquitous Security (UbiSec 2024)*, 29-31 December 2024, Changsha, China.
2. Keynote, “Private service discovery and intelligent batch authentication in IoT networks”, *Cyber Security and Trustworthy Systems Researchers Meet*, 11-12 November 2024, University of New South Wales, Sydney.
3. Keynote, “Post-quantum cryptography – research and migration”, *The 2nd International Conference on Data Security and Privacy Protection (DSPP 2024)*, 25-28 October 2024, Xi’an, China.
4. Keynote, “Toward practical client-side encryption in cloud computing”, *The 19th ACM ASIA Conference on Computer and Communications Security (ASIACCS 2024)*, 1-5 July 2024, Singapore.
5. Keynote, “TEE-assisted crypto systems – towards designing practical data security solutions”, *25th International Conference on Information and Communications Security (ICICS 2023)*, 18-20 November 2023, Tianjin, China.
6. Keynote, “Towards practical multiuser searchable encryption”, *The 2nd International Workshop on Cyber Security (CSW 2023)*, 13-15 October 2023, Hangzhou, China
7. Keynote, “Hardware-assisted data security & privacy solutions”, *19th EAI International Conference on Security and Privacy in Communications Networks (SecureComm 2023)*, 19-20 October 2023, Hong Kong.
8. Keynote, “Data security & privacy protection in IoT MGC systems”, *The 9th ACM Cyber-Physical System Security Workshop (CPSS 2023)*, Melbourne, VIC, Australia, July 10-14, 2023.
9. Keynote, “Efficiently deployable and efficiently searchable encryption – applications, attacks, and countermeasures”, the 16th International Conference on Network and System Security (NSS 2022), Denarau Island, Fiji, 9-12 December 2022.
10. Keynote, “Efficiently deployable and efficiently searchable encryption – applications, attacks, and countermeasures”, *Information Security Conference (ISC 2022)*, Bali, Indonesia, 18-22 December 2022.
11. Keynote, “Protecting cloud data security and privacy through encryption”, *the 17th International Conference on Information Security Practice and Experience (ISPEC 2022)*, Taipei, Taiwan, 23-25 November 2022.
12. Keynote, “Achieving cloud data security and privacy in zero trust environments”, *2022 IEEE Cybermatics Congress*, Espoo, Finland, 22-25 August 2022.
13. Keynote, “AI security threats, compliance, and standards”, *Industrial Forum of Artificial Intelligence-Driven Future, Global Digital Economy Conference 2022* (2022全球数字经济大会) 28 – 30 July 2022, Beijing, China.
14. Keynote, “Secure cloud data storage for enterprise users – from cryptographic research to system design”, *EAI International Conference on Applied Cryptography in Computer and Communications (AC3 2021)*, 15-16 May 2021, Xiamen, China.
15. Keynote, “Privacy-preserving deep packet inspection on TLS traffic”, the *14th International Conference on Network and System Security*, 25-27 November 2020, Melbourne, Australia.
16. Keynote, “Towards leakage resilient user authentication”, the *21st International Conference on Information and Communications Security*, 15-17 December 2019, Beijing, China
- 17.

18. Keynote, “When seeing is not believing – defeating spoofing attacks in face authentication in mobile platforms”, *the 15th International Conference on Information Security and Cryptology*, 6-8 December 2019, Nanjing, China.
19. Invited talk, “Finding implementation flaws in password and OTP authentication code in Android apps”, *2019 Huawei Forum on Future Security*, 25 November 2019, Kuala Lumpur, Malaysia.
20. Keynote, “Long road towards secure and usable password authentication”, *the 2019 IEEE Conference on Dependable and Secure Computing*, 18-20 November 2019, Hangzhou, China.
21. Keynote, “Secure sharing and computation of encrypted data in untrusted servers”, *Cyber Security Summer School 2019*, Data61/CSIRO and Defence Science and Technology Group, 21-22 March 2019, Adelaide, Australia.
22. Keynote, “Protecting data security and privacy in untrusted servers”, *the 14th International Conference on Information Security and Cryptology (Inscrypt 2018)*, 14-16 December 2018, Fuzhou, China.
23. Keynote, “New cryptographic techniques for data security and privacy protection in the cloud”, *Huawei Connect*, 10-12 October 2018, Shanghai, China
24. Keynote, “A user centric and layered approach to mobile security”, *the 14th International Conference on Information Security Practice and Experience (ISPEC 2018)*, 25-27 September 2018, Tokyo, Japan
25. Invited talk, “End-to-end secure mobile computing in the Internet of Things”, *the 23rd European Symposium on Research in Computer Security (ESORICS 2018)*, 3-7 September 2018, Barcelona, Spain
26. Keynote, “A user centric approach to secure mobile systems and applications”, *the 14th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2018)*, 8-10 August 2018, Singapore
27. Keynote, “Strengthening the weakest links in IoT security”, *the 23rd Australasian Conference on Information Security and Privacy (ACISP 2018)*, 11-13 July 2018, Wollongong, Australia.
28. Keynote, “Present and future challenges in IoT security”, *ACM SIGSAC China Symposium, ACM Turing Celebration Conference (ACM TURC 2018)*, 19-20 May 2018, Shanghai, China.
29. Invited Talk, “Present and future challenges in IoT Security”, *Huawei Strategy and Technology Workshop*, 15-16 May 2018, Shenzhen, China
30. Invited Talk, “Bitcoin, blockchain and smart contract”, *IT Development Talk to Supreme Court Judges*, 6 March 2018, Singapore.
31. Keynote, “Privacy-preserving access control and computations of encrypted data in the cloud”, *The 10th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS 2017)*, 12-15 Dec 2017, Guangzhou, China.
32. Invited talk, “A layered approach to secure mobile computing”, *Cyber Week 2017 – Academic Track*, 25-29 June 2017, Tel Aviv, Israel.
33. Keynote, “Performance and cryptographic key management for mobile users in secure cloud storage systems”, *the 3rd International Symposium on Mobile Security (MSEC 2016)*, 9 December, Seoul, Korea.
34. Keynote, “Achieving end-to-end security in mobile computing”, *The 21st ACM Symposium on Access Control Models and Technologies*, 6-8 June, 2016, Shanghai, China
35. Keynote, “Attribute-based encryption for access control of encrypted data in the cloud”, *the 4th International Workshop on Security and Forensics in Cyber Space (SFCS 2016)*, in

- conjunction with the 17th International Conference on Distributed Computing and Networking (ICDCN 2016), 4-6 January 2016, Singapore
36. Invited speech, “Achieving data security & privacy in untrusted servers”, *Fudan Science and Innovation Forum*, 17th-18th December, 2015, Shanghai, China.
 37. Keynote. Flexible and scalable search and sharing of encrypted data in the cloud, the 7th International Conference on Trusted Systems (Intrust2015), 7th-8th December, 2015, Beijing.
 38. Keynote. Efficient and privacy-preserved sharing of encrypted data in the cloud”, the The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE Trustcom’15), 20-22 August, 2015. Helsinki, Finland.
 39. Invited talk “Secure Mobile Centre at Singapore Management University”, *Financial Services Information Security Forum*, Association of Banks in Singapore, 3 August 2015
 40. Distinguished Lecture. Protecting security and privacy of outsourced data in the cloud”, *The Croucher Foundation Advanced Study Institute – Information Security and Privacy in Social Networks and Cloud Computing*, 2-4 December 2014, Hong Kong.
 41. Keynote speech, “Scalable access control & sharing of encrypted data in the cloud”, *International Conference on Cloud Computing Research and Innovation*, 27-28 October 2014, Singapore.
 42. Invited talk, “Towards scalable and secure sharing of encrypted data in the cloud”, *Governmentware 2014*, 23-25 September 2014, Singapore.
 43. Invited talk. Towards secure and usable user authentication in e-banking and e-payment”, *2014 Huawei Strategy and Technology Workshop*, 13-15 May 2014, Shenzhen, China.
 44. Keynote speech. RFID security & privacy –recent developments & challenges”, *The 2013 Workshop on RFID and IoT Security (RFIDsec’13 Asia)*, 27 November 2013, Guangzhou, China.
 45. Invited Tutorial. Robert H. Deng, “Flexible access control of encrypted data in the cloud”, *The 6th International Conference on Pairing-Based Cryptography (Pairing 2013)*, 22-24 November, 2013, Beijing, China.
 46. Keynote speech. Secure access to outsourced data”, *The 2013 International Workshop on Security in Cloud Computing, Co-located with AsiaCCS2013*, May 8, 2013, Hangzhou, China.
 47. Keynote speech. Access control of encrypted data in untrusted servers”, the The 4th International Symposium on Cyberspace Safety and Security (CSS 2012), 12-13 December 2012, Melbourne, Australia.
 48. Invited Talk. Robert H. Deng, “On limitations of designing leakage-resilient password systems”, *Coding and Cryptography Research Group Seminar*, Nanyang Technological University, 25th November 2011.
 49. Invited Talk. Robert H. Deng and Yingjiu Li, “RFID security and privacy at both physical and system levels”, *Internet of Things –Global Standards Initiative (IoT-GSI) Meeting*, International Telecommunications Union (ITU), 22-26 August 2011, Geneva, Switzerland.
 50. Invited Talk. R. H. Deng, “Some recent development in RFID privacy models”, *French-German-Singaporean Workshop on Applied Cryptography*, Jointly organized by NTU, German Academic Exchange Service DAAD, the Embassies of France and Germany, 2 & 3 December 2010.
 51. Keynote Speech. Detecting node clones in wireless sensor networks”, *The 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010)*, 7-9 September 2010, Singapore.

52. Keynote Speech. RFID privacy models and a minimal condition”, *The 5th China International Conference on Information Security and Cryptology (INSCRYPT 2009)*, 12-15 December 2009, Beijing, China.
53. Keynote Speech. Scalable end-to-end multimedia content authentication techniques”, *The 2009 International Conference on Multimedia Information Networking and Security (MINES 2009)*, 18-20 November 2009, Wuhan, China.
54. Keynote Speech. The future of password”, *The 19th Cryptology and Information Security Conference*, Taipei, Taiwan, 4th -5th June 2009.
55. Invited Talk. R. H. Deng, “Innovative and practical applications of cryptography”, School of Computer Science and Technology, Xidian University, Xi’an, China, 14th April 2009.
56. Invited Talk. R. H. Deng, “Achieving strong user authentication using weak secret”, *Information Security Seminar for Mindef/DSTA*, organized by ST Electronics (Info-Security), 29th August 2008.
57. Keynote Speech. Scalable authentication techniques compatible with modern multimedia coding standards”, *The Fourth Information Security Practice and Experience Conference (ISPEC2008)*, 21st-23rd April 2008, Sydney, Australia.
58. Invited Lecture. R. H. Deng, “Innovative applications of trusted computing platform”, The First Asia-Pacific Summer School on Trusted Infrastructure Technologies, 20th – 24th August 2007, Zhuhai, China
59. Invited lecture. R. H. Deng, “Techniques for trusted electronic transactions”, *2007 Information Security Summer School, Taiwan Information Security Center*, 6th – 16th August 2007, Taipei, Taiwan.
60. Keynote Speech. Towards efficient and novel security solutions - a marriage of crypto and trusted computing platform”, *The 3rd Information Security Practice and Experience Conference (ISPEC2007)*, 7th-9th May, 2007, Hong Kong, China.
61. Invited Talk. R. H. Deng, “Cryptography and Innovative Applications”, 7th March 2007, College of Computer Science and Technology, Wuhan University, China.
62. Plenary Lecture. R. H. Deng, “Towards practical private information retrieval”, *The 1st International Conference on Information Security and Computer Forensics (ISCF’06)*, 6th-8th December 2006, Chennai, India.
63. Invited Speech. R. H. Deng, “Recent advances in privacy protection in database applications”, *The 2nd National Conference on Cryptology (NCC’06)*, 28th-29th November 2006, Kuala Lumpur, Malaysia.
64. Keynote speech. R. H. Deng, “Inference control and private information retrieval – two sides of one tapestry”, *The 4th International Conference on Applied Cryptography and Network Security (ACNS’06)*, 6th-9th June, 2006, Singapore.
65. Invited Talk. New developments in security systems and cryptographic applications”, *The Croucher Foundation Advanced Study Institute – Cryptography and Wireless Security*, 11th-16th December 2004, City University of Hong Kong.
66. Invited Talk. R. H. Deng, “Cryptographic approach to modern multimedia content security”, 19th October 2004, Department of Computer Science and Engineering, Shanghai Jiaotong University, China.
67. Invited talk. R. H. Deng, “Privacy enhanced super-distribution of multimedia content”, The 7th Sept., 2004, CyLab Seminar, Carnegie Mellon University, USA.
68. Invited talk. R. H. Deng, “Challenges in securing mobile IP”, *Workshop on Mobile, Wireless and Sensor Networks: Technology and Future Directions*, sponsored by BSIG, Cisco Systems,

IBM, IEEE, NUS, and Pearson,, 5th-6th March 2004.

69. Invited talk. R. H. Deng, “Securing JPEG2000 – the next generation image compression standard”, *Workshop on Advanced Developments in Software and Systems Security*, sponsored by UC Berkeley, Academia Sinica, National Chiao Tung University, IEEE Taipei Section and the Chinese Cryptology and Information Security Association, 5th-7th December 2003, Taipei, Taiwan.
70. Invited speaker. R. H. Deng, “Security challenges in ubiquitous computing”, *Annual Meeting of the Korea Institute for Information Security and Cryptology*, 21st February 2003, Pohang, Korea.
71. Invited talk. R. H. Deng, “Defending against redirect attacks in mobile IP”, *Mathematics Department and Temasek Labs joint seminar on Coding/Crypto/Combinatorics*, 16th October 2002, National University of Singapore.
72. Invited talk. R. H. Deng, “Enabling information security technologies”, organized by *Bioinformatics Institute*, Singapore, 4th October 2002.
73. Invited keynote and panel discussion. R. H. Deng, Bao Feng, and Karen Worstell, “What's over the horizon? New technologies to watch”, *The 43rd International Information Integrity Institute Forum*, 11th-13th June 2001, Berlin, German.
74. Invited talk. R. H. Deng, “Overview of internet security issues and technologies“, *Workshop on Internet Security and e-Commerce*, organized by Shanghai City Information Technology Office and Computer Center, 14th December 2000, Shanghai, China.
75. Panel discussion. R. H. Deng, Panel discussion at *Removing the Barriers to e-Business - Net Present Value of Security: CEO Luncheon Briefing*, organized by AtomicTangerine and Forbes, 11th October 2000, Gibson Hall, London.
76. Invited talk. R. H. Deng, “Virtual private network standards and technologies”, *Secure e-Business Internet Infrastructure Symposium*, organized by the Chinese Academy of Sciences and Internet Appliance, Inc, 12th September 2000, Beijing, China.
77. Invited talk. R. H. Deng, “Virtual private networks in remote access”, *Mobile/Remote Access Network and Platform Challenges: Extending the Boundaries of Business Conference*, 22nd-24th March 2000, New Orleans, Louisiana.
78. Invited talk. R. H. Deng, “Information security R&D at Kent Ridge Digital Labs”, *The 6th ACM Conference on Computer and Communications Security*, 2nd-4th November 1999, Singapore.

9 Graduated PhD Students

- Yang Yanjiang, “Ensuring data security and individual privacy in health care systems”, PhD Thesis, NUS, 2006
- Wan Zhiguo, “Authentication and key establishment in wireless networks”, PhD Thesis, NUS, 2006
- Zhu Bo, “Security and privacy for large ad-hoc networks”, PhD Thesis, NUS, 2006
- Yan Qiang, “Towards secure and usable leakage-resilient password entry”, PhD Thesis, SMU, 2013.
- Cheng Yueqiang, “Virtualization-based system hardening against untrusted kernels”, PhD Thesis, SMU, 2013.
- Cai Shaoying (co-advisor), “Security and privacy in RFID-enabled supply chains”, PhD Thesis, SMU, 2015.
- Lo Swee Won, “Towards secure online distribution of multimedia codestreams”, PhD Thesis,

SMU, 2015.

- Kywe Su Mon (co-advisor), “Techniques for identifying mobile platform vulnerabilities and detecting policy-violating applications”, SMU, 2016.
- Xu Ke, “Advanced malware detection for Android platform”, PhD Thesis, SMU, 2018.
- Ma Siqu, “Automatic vulnerability detection and repair”, PhD Thesis, SMU, 2018.
- Liu Ximing (co-advisor), “When keystroke meets password: attacks and defenses”, SMU, 2019.
- Tang Xiaoxiao (co-advisor), “Sensitive behavior analysis of Android applications on unrooted devices in the wild”, SMU, 2019.
- Wu Daoyuan (co-advisor), “On-the-fly Android static analysis with applications in vulnerability discovery”, SMU, 2019.
- Hong Jiaqi (co-advisor), “A virtualization-based system infrastructure for dynamic program analysis”, PhD Thesis, SMU, 2020.
- Xu Jiayun, “Machine learning based approaches towards robust Android malware detection”, PhD Thesis, SMU, 2021.

10 Postdoctoral Fellows Supervised

- Chu Cheng-Kang, Cui Hui, Ding Wenxiu, Hao Meng, Hung Xinyi, Lai Junzhuo, Li Feng, Li Ming, Li Xiaoguo, Liu Ximeng, Ma Changshe, Ma Jinhua, Ning Jianting, Qin Baodong, Shi Jie, Sun Jianfei, Wang Shuhong, Wan Zhiguo, Wei Zhuo, Weng Jian, Wu Pengfei, Xu Guowen, Xu Shengmin, Yang Yanjiang, Yang Yang, Yao Lisha, Zhang Yinghui, Zhao Bowen, Zhao Yunlei, Zhu Wentao.