**Robert H DENG**

School of Computing and Information Systems
Singapore Management University (SMU)
80 Stamford Road
Singapore 178902

Email: robertdeng@smu.edu.sg
Office Phone: +65 68280920

## Education

PhD, Illinois Institute of Technology, United States of America, 1985

Master of Science, Illinois Institute of Technology, United States of America, 1983

Bachelor of Engineering, National University of Defence Technology, China, 1981

## Academic Appointments

AXA Chair Professor of Cybersecurity, School of Computing and Information Systems, SMU, Mar 2017 - Present

Professor of Information Systems, School of Computing and Information Systems, SMU, Jul 2004 - Mar 2017

Senior Lecturer, Department of Electrical and Computer Engineering, National University of Singapore, Singapore, Jul 1991 - Jun 1994

Postdoctoral Research Associate, University of Notre Dame, United States of America, Jan 1986 - Jun 1987

## Academic Administrative Positions

Director, Secure Mobile Centre, National Satellite of Excellence in Mobile Systems Security & Cloud Security, SMU, Jul 2023 - Present

Deputy Dean, Faculty & Research, School of Computing and Information Systems, SMU, Jul 2018 - Present

Dean, College of Graduate Research Studies, SMU, Sep 2016 - Jun 2018

Director, Secure Mobile Centre, Secure Mobile Centre, SMU, Feb 2015 - Present

Associate Dean (Faculty), School of Computing and Information Systems, SMU, Jul 2012 - Jun 2015

Director, SCIS Research Centre (External Funded), SMU, Aug 2004 - Jun 2012

Director, SCIS Research Centre (External Funded), SMU, Jul 2004 - Jun 2008

Senior Research Staff Member and Manager of Information Security Group, Institute of System Science, National University of Singapore, Singapore, Jan 1994 - Jan 1998

Research Staff Member and Project Leader of Communications Group, Institute of Systems Science, National University of Singapore, Singapore, Jul 1987 - Jun 1991

## Other Positions and Affiliations

Principle Scientist and Department Manager, Institute for Infocomm ResearchInfocomm Security Department, Agency for Science, Technology and Research (A*STAR), Singapore, Apr 2002 - Jun 2004

Principal Research Staff Member and Director (Ubiquitous and Distributed Computing Program), Lab for Information Technology, A*STAR, Singapore, Apr 2001 - Mar 2002

Principal Research Staff Member and Deputy Director of Ubiquity Lab, Kent Ridge Digital Labs, National Science and Technology Board, Singapore, Jan 1998 - Mar 2001

### Awards and Honors

Outstanding Paper Award, 21st IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2022), 2022

Best Paper Award, IEEE Conference on Dependable and Secure Computing (IEEE DSC 2022), 2022

The Public Administration Medal (Silver), Singapore National Day Awards 2020, 2020

Best Paper, 25th European Symposium on Research in Computer Security (ESORICS) 2020, 2020

Fellow, Academy of Engineering Singapore, 2019

2017 Best Journal Paper Award, IEEE Communications Society, Big Data Technical Committee, 2017

Huawei Distinguished Collaboration Project Award, Shield Lab, Huawei, 2016

Fellow, IEEE, 2016

Best Paper Award, The 13th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2012), Canterbury, UK., International Federation for Information Processing, 2012

Distinguished Paper Award, The 19th Network and Distributed System Security Symposium (NDSS 2012), San Diego, USA., Internet Society, 2012

Asia-Pacific Information Security Leadership Achievements (ISLA) Community Service Star and Showcased Senior Information Security Professional, International Information Systems Security Certification (ISC)2), 2010, (ISC)2, 2010

Lee Kuan Yew Fellow for Research Excellence,2006., Singapore Management University, 2005

Role Model for the category of Principal Research Staff Member, Singapore, 2002., Laboratories for Information Technology, 2002

University Outstanding Researcher Award, Singapore, November 1999., National University of Singapore, 1999

Excellent Graduate Certificate, National University of Defense Technology, China, December 1981., National University of Defense Technology, 1982

## RESEARCH

### Publications

Journal Articles [Refereed]

Privacy-Preserving Bloom Filter-Based Keyword Search Over Large Encrypted Cloud Data, by LIANG, Yanrong; MA, Jianfeng; MIAO, Yinbin; KUANG, Da; MENG, Xiangdong; DENG, Robert H.. (2023). *IEEE Transactions on Computers, 72* (11), 3086-3098. https://doi.org/10.1109/TC.2023.3285103 (Published)

Privacy-preserving arbitrary geometric range query in mobile Internet of Vehicles, by MIAO, Yinbin; SONG,

Lin; LI, Xinghua; LI, Hongwei; CHOO, Kim-Kwang Raymond; DENG, Robert H.. (2023). *IEEE Transactions on Mobile Computing,* 1-15. https://doi.org/10.1109/TMC.2023.3336621 (Advance Online)

STDA: Secure Time Series Data Analytics with practical efficiency in wide-area network, by LI, Xiaoguo; HUANG Zixi; ZHAO, Bowen; YANG, Guomin; XIANG, Tao; DENG, Robert H.. (2023). *IEEE Transactions on Information Forensics and Security, 19* 1440-1454. (Published)

Policy-Based Remote User Authentication From Multi-Biometrics, by TIAN, Yangguang; LI, Yingjiu; DENG, Robert H.; YANG, Guomin; LI, Nan. (2023). *Computer Journal,* https://doi.org/10.1093/comjnl/bxad102 (Advance Online)

Owner-free Distributed Symmetric Searchable Encryption supporting Conjunctive queries, by TONG, Qiuyun; LI, Xinghua; MIAO, Yinbin; WANG, Yunwei; LIU, Ximeng; DENG, Robert H.. (2023). *Transactions on Storage, 19* (4), 1-25. https://doi.org/10.1145/3607255 (Published)

PRI: PCH-based privacy-preserving with reusability and interoperability for enhancing blockchain scalability, by LI, Yuxian; WENG, Jian; WU, Wei; LI, Ming; LI, Yingjiu; TU, Haoxin; WU, Yongdong; DENG, Robert H.. (2023). *Journal of Parallel and Distributed Computing, 180* 1-15. https://doi.org/10.1016/j.jpdc.2023.104721 (Published)

A Causality-Aligned Structure Rationalization Scheme Against Adversarial Biased Perturbations for Graph Neural Networks, by JIA, Ju; MA, Siqi; LIU, Yang; WANG, Lina; DENG, Robert H.. (2024). *IEEE Transactions on Information Forensics and Security, 19* 59-73. https://doi.org/10.1109/TIFS.2023.3318936 (Published)

Hercules: Boosting the performance of privacy-preserving federated learning, by XU, Guowen.; HAN, Xingshuo.; XU, Shengmin.; ZHANG, Tianwei.; LI, Hongwei.; HUANG, Xinyi.; DENG, Robert H.. (2023). *IEEE Transactions on Dependable and Secure Computing, 20* (5), 4418-4433. (Published)

Fair cloud auditing based on blockchain for resource-constrained IoT devices, by ZHOU, Lei.; FU, Anmin.; YANG, Guomin.; GAO, Yansong.; YU, Shui.; DENG, Robert H.. (2023). *IEEE Transactions on Dependable and Secure Computing, 20* (5), 4325-4342. https://doi.org/10.1109/TDSC.2022.3207384 (Published)

Fair Cloud Auditing based on Blockchain for resource-constrained IoT devices, by ZHOU, Lei; FU, Anmin; YANG, Guomin; GAO, Yansong; YU, Shui; DENG, Robert H.. (2023). *IEEE Transactions on Dependable and Secure Computing, 20* (5), 4325-4342. https://doi.org/10.1109/TDSC.2022.3207384 (Published)

Efficient Privacy-Preserving Federated Learning With Improved Compressed Sensing, by ZHANG, Yifan.; MIAO, Yinbin.; LI, Xinghua.; WEI, Linfeng.; LIU, Zhiquan,; CHOO, Kim-Kwang R.; DENG, Robert H.. (2023). *IEEE Transactions on Industrial Informatics,* https://doi.org/10.1109/TII.2023.3297596 (Advance Online)

Privacy-Preserving Multi-User Outsourced Computation for Boolean Circuits, by LIU, Xueqiao.; YANG, Guomin.; SUSILO, Willy.; HE, Kai.; DENG, Robert H.; WENG, Jian.. (2023). *IEEE Transactions on Information Forensics and Security, 18* 4929-4943. (Published)

CROWDFL: Privacy-Preserving Mobile Crowdsensing System Via Federated Learning, by ZHAO, Bowen; LIU, Ximeng; CHEN, Wei-Neng; DENG, Robert H.. (2023). *IEEE Transactions on Mobile Computing, 22* (8), 4607-4619. https://doi.org/10.1109/TMC.2022.3157603 (Published)

Privacy-Preserving Asynchronous Federated Learning Framework in Distributed IoT, by YAN, Xinru; MIAO, Yinbin; LI, Xinghua; CHOO, Kim-Kwang Raymond; MENG, Xiangdong; DENG, Robert H.. (2023). *IEEE Internet of Things Journal, 10* (15), 13281-13291. https://doi.org/10.1109/JIOT.2023.3262546 (Published)

PAM<SUP>3</SUP>S: Progressive Two-Stage Auction-Based Multi-Platform Multi-User Mutual Selection Scheme in MCS, by LUO, Bin; LI, Xinghua; MIAO, Yinbin; ZHANG, Man; LIU, Ximeng; REN, Yanbing; LUO, Xizhao; DENG, Robert H.. (2023). *IEEE/ACM Transactions on Networking,* 1-16. https://doi.org/10.1109/TNET.2023.3297258 (Advance Online)

Comprehensive Survey on Privacy-Preserving Spatial Data Query in Transportation Systems, by MIAO, Yinbin; YANG, Yutao; LI, Xinghua, CHOO, Kim-Kwang Raymond; MENG, Xiangdong; DENG, Robert H.. (2023). *IEEE Transactions on Intelligent Transportation Systems,* 1-14. https://doi.org/10.1109/TITS.2023.3295798 (Advance Online)

Privacy-Aware and Security-Enhanced Efficient Matchmaking Encryption, by SUN, Jianfei; XU, Guowen; ZHANG, Tianwei; YANG, Xuehuan; ALAZAB, Mamoun; DENG, Robert H.. (2023). *IEEE Transactions on Information Forensics and Security, 18* 4345-4360. https://doi.org/10.1109/TIFS.2023.3294725 (Published)

Forward/Backward and Content Private DSSE for Spatial Keyword Queries, by WANG, Xiangyu; MA, Jianfeng; LIU, Ximeng; MIAO, Yinbin; LIU, Yang; DENG, Robert H.. (2023). *IEEE Transactions on Dependable and Secure Computing, 20* (4), 3358-3370. https://doi.org/10.1109/TDSC.2022.3205670 (Published)

FeSA: Automatic Federated Swarm Attestation on Dynamic Large-Scale IoT Devices, by KUANG, Boyu; FU, Anmin; GAO, Yansong; ZHANG, Yuqing; ZHOU; Jianying; DENG, Robert H.. (2023). *IEEE Transactions on Dependable and Secure Computing, 20* (4), 2954-2969. https://doi.org/10.1109/TDSC.2022.3193106 (Published)

ACB-Vote: Efficient, Flexible, and Privacy- Preserving Blockchain-Based Score Voting With Anonymously Convertible Ballots, by XUE, Wenyi, YANG, Yang; LI, Yingjiu; PANG, Hwee Hwa; DENG, Robert H.. (2023). *IEEE Transactions on Information Forensics and Security, 18* 3720-3734. https://doi.org/10.1109/TIFS.2023.3287394 (Published)

MP-CLF: An effective model-preserving collaborative deep learning framework for mitigating data leakage under the GAN, by CHEN, Zhenzhu; WU, Jie; FU, Anmin; SU, Mang; DENG, Robert H.. (2023). *Knowledge-Based Systems, 270* (C), 1-13. https://doi.org/10.1016/j.knosys.2023.110527 (Published)

LiVoAuth: Liveness Detection in Voiceprint Authentication With Random Challenges and Detection Modes, by ZHANG, Rui; YAN, Zheng; WANG, Xueru; DENG, Robert H.. (2023). *IEEE Transactions on Industrial Informatics, 19* (6), 7676-7688. https://doi.org/10.1109/TII.2022.3213830 (Published)

Privacy-Preserving Ranked Spatial Keyword Query in Mobile Cloud-Assisted Fog Computing, by Tong QY, Miao YB, Li HW, Liu XM, Deng RH. (2023). *IEEE Transactions on Mobile Computing, 22* (6), 3604-3618. https://doi.org/10.1109/TMC.2021.3134711 (Published)

Threshold attribute-based credentials with redactable signature, by SHI, Rui; FENG, Huamin; YANG, Yang; YUAN, Feng; LI, Yingjiu; PANG, Hwee Hwa; DENG, Robert H.
. (2023). *IEEE Transactions on Services Computing, 16* (5), 3751-3765. https://doi.org/10.1109/TSC.2023.3280914 (Published)

Identifiable, But Not Visible: A Privacy-Preserving Person Reidentification Scheme, by ZHAO, Bowen; LI, Yingjiu; LIU, Ximeng; LI, Xiaoguo; PANG, Hwee Hwa; DENG, Robert H. . (2023). *IEEE Transactions on Reliability,* 1-13. https://doi.org/10.1109/TR.2023.3258983 (Published)

VOLERE: Leakage resilient user authentication based on personal voice challenges, by ZHANG, Rui; YAN, Zheng; WANG, Xuerui; DENG, Robert H.. (2023). *IEEE Transactions on Dependable and Secure Computing, 20* (2), 1002-1016. https://doi.org/10.1109/TDSC.2022.3147504 (Published)

Accountable and Fine-Grained Controllable Rewriting in Blockchains, by XU, Shengmin; HUANG, Xinyi; YUAN, Jiaming; LI, Yingjiu; DENG, Robert H.. (2023). *IEEE Transactions on Information Forensics and Security, 18* 101-116. https://doi.org/10.1109/TIFS.2022.3217742 (Published)

CrowdFA: A Privacy-Preserving Mobile Crowdsensing Paradigm via Federated Analytics, by ZHAO, Bowen; LI, Xiaoguo; LIU, Ximeng; PEI, Qingqi; LI, Yingjiu; DENG, Robert H.. (2023). *IEEE Transactions on Information Forensics and Security, 18* 5416-5430. https://doi.org/10.1109/TIFS.2023.3308714 (Published)

VerifyTL: Secure and Verifiable Collaborative Transfer Learning, by MA, Zhuoran; MA, Jianfeng; MIAO, Yinbin; LIU, Ximeng; ZHENG, Wei; CHOO, Kim-Kwang Raymond; DENG, Robert H.. (2023). *IEEE Transactions on Dependable and Secure Computing,* 1-14. https://doi.org/10.1109/TDSC.2023.3241181 (Advance Online)

A secure EMR sharing system with tamper resistance and expressive access control, by XU, Shengmin; NING, Jianting; LI, Yingjiu; ZHANG, Yinghui; XU, Guowen; HUANG, Xinyi; DENG, Robert H. (2023). *IEEE Transactions on Dependable and Secure Computing, 20* (1), 53-67. https://doi.org/10.1109/TDSC.2021.3126532 (Published)

Verifiable, Fair and Privacy-Preserving Broadcast Authorization for Flexible Data Sharing in Clouds, by SUN, Jianfei; XU, Guowen; ZHANG, Tianwei; YANG, Xuehan; ALAZAB, Mamoun; DENG, Robert H.. (2023). *IEEE Transactions on Information Forensics and Security, 18* 683-698. https://doi.org/10.1109/TIFS.2022.3226577 (Published)

Authenticable Data Analytics Over Encrypted Data in the Cloud, by CHEN, Lanxing; MU, Yi; ZENG, Lingfang; REZAEIBAGHA, Fatemah; DENG, Robert H.. (2023). *IEEE Transactions on Information Forensics and Security, 18* https://doi.org/10.1109/TIFS.2023.3256132 (Advance Online)

Intelligent adaptive gossip-based broadcast protocol for UAV-MEC using multi-agent deep reinforcement learning, by REN, Zen; LI, Xinghua; MIAO, Yinbin; LI, Zhuowen; WANG, Zihao; ZHU, Mengyao; LIU, Ximeng; DENG, Robert H.. (2023). *IEEE Transactions on Mobile Computing,* 1-17. https://doi.org/0.1109/TMC.2023.3323296 (Published)

OpenSE: Efficient verifiable searchable encryption with access and search pattern hidden for Cloud-IoT, by YANG, Yunbo; HU, Yiwei; DONG, Xiaolei; SHEN, Jiachen; CAO, Zhenfu; YANG, Guomin; DENG, Robert H.. (2023). *IEEE Internet of Things Journal, 1* 1-15. https://doi.org/10.1109/JIOT.2023.3337336 (Advance Online)

REKS: Role-based Encrypted Keyword Search with enhanced access control for outsourced cloud data, by MIAO, Yibin; LI, Feng; JIA, Xiaohua; WANG, Huaxiong; LIU, Ximeng; CHOO, Kim-Kwang Raymond; DENG, Robert H.. (2023). *IEEE Transactions on Dependable and Secure Computing,* 1-15. https://doi.org/10.1109/TDSC.2023.3324640 (Advance Online)

A secure and robust knowledge transfer framework via stratified-causality distribution adjustment in intelligent collaborative services, by JIA, Ju; MA, Siqi; WANG, Lina; LIU, Yang; DENG, Robert H.. (2023). *IEEE Transactions on Computers,* 1-14. https://doi.org/10.1109/TC.2023.3318403 (Advance Online)

SOCI: A Toolkit for Secure Outsourced Computation on Integers, by ZHAO, Bowen; YUAN, Jiaming; LIU, Ximeng; WU, Yongdong; PANG, Hwee Hwa; DENG, Robert H.. (2022). *IEEE Transactions on Information Forensics and Security, 17* 3637-3648. http://doi.org/10.1109/TIFS.2022.3211707 (Published)

Structured encryption for knowledge graphs, by XUE, Yujie; CHEN, Lanxiang; MI, Yu; ZENG, Lingfang; REZAEIBAGHA, Fatemeh; DENG, Robert H. . (2022). *Information Sciences, 605* 43-70. http://doi.org/10.1016/j.ins.2022.05.015 (Published)

Time-Controlled Hierarchical Multikeyword Search Over Encrypted Data in Cloud-Assisted IoT, by LIU, Tong; MIAO, Yinbin; CHOO, Kim-Kwang Raymond; LI, Hongwei; LIU, Ximeng; MENG, Xiangdong; DENG, Robert H. (2022). *IEEE Internet of Things Journal, 9* (13), 11017-11029. http://doi.org/10.1109/JIOT.2021.3126468 (Published)

Sanitizable Access Control System for Secure Cloud Storage Against Malicious Data Publishers, by SUSILO, Willy; JIANG, Peng; LAI, Jianchang; GUO, Fuchun; YANG, Guomin; DENG, Robert H.. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (3), 2138-2148. https://doi.org/10.1109/TDSC.2021.3058132 (Published)

Verifiable Searchable Encryption Framework Against Insider Keyword-Guessing Attack in Cloud Storage, by MIAO, Yinbin; DENG, Robert H.; CHOO, Kim-Kwang Raymond; LIU, Ximeng; LI, Hongwei. (2022). *IEEE Transactions on Cloud Computing, 10* (2), 835-848. https://doi.org/10.1109/TCC.2020.2989296 (Published)

SDAC: A Slow-Aging Solution for Android Malware Detection Using Semantic Distance Based API Clustering, by XU, Jiayun; LI Yingjiu; DENG, Robert H.; XU, Ke. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (2), 1149-1163. https://doi.org/10.1109/TDSC.2020.3005088 (Published)

Privacy-Preserving Federated Deep Learning With Irregular Users, by XU, Guowen; LI, Hongwei; ZHANG, Yun; XU, Shengmin; NING, Jianting; DENG, Robert H.. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (2), 1364-1381. https://doi.org/10.1109/TDSC.2020.3005909 (Published)

Lightweight Privacy-Preserving GAN Framework for Model Training and Image Synthesis, by YANG, Yang; MU, Ke; DENG, Robert H.. (2022). *IEEE Transactions on Information Forensics and Security, 17* 1083-1098. https://doi.org/10.1109/TIFS.2022.3156818 (Published)

Update Recovery Attacks on Encrypted Database Within Two Updates Using Range Queries Leakage, by NING, Jianting; POH, Geong Sen; HUANG, Xinyi; DENG, Robert H.; CAO, Shuwei; CHANG, Ee Chien. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (2), 1164-1180. https://doi.org/10.1109/TDSC.2020.3015997 (Published)

Towards Privacy-Preserving Spatial Distribution Crowdsensing: A Game Theoretic Approach, by REN, Yanbing; LI, Xinghua; MIAO, Yinbin; LUO, Bin; WENG, Jian; CHOO, Kim-Kwang Rahmond; DENG, Robert H.. (2022). *IEEE Transactions on Information Forensics and Security, 17* 804-818. https://doi.org/10.1109/TIFS.2022.3152409 (Published)

PrivacySignal: Privacy-Preserving Traffic Signal Control for Intelligent Transportation System, by YING, Zuobin; CAO, Shuanglong; LIU, Ximeng; MA, Zhuo; MA, Jianfeng; DENG, Robert H.. (2022). *IEEE Transactions on Intelligent Transportation Systems, 23* (9), 16290 -16303.

https://doi.org/10.1109/TITS.2022.3149600 (Published)

Verifiable Data Mining Against Malicious Adversaries in Industrial Internet of Things, by MA, Zhuoran; MA, Jianfeng; MIAO, Yinbin; LIU, Ximeng; CHOO, Kim-Kwang Raymond; GAO, Yu; DENG, Robert H. (2022). *IEEE Transactions on Industrial Informatics, 18* (2), 953-964. https://doi.org/10.1109/TII.2021.3077005 (Published)

Orchestration or Automation: Authentication Flaw Detection in Android Apps, by MA, Siqi; LI, Juanru; NEPAL, Surya; OSTRY, Diethelm; LO, David; JHA, Sanjay K.; DENG, Robert H.; BERTINO, Elisa. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (4), 2165-2178. https://doi.org/10.1109/TDSC.2021.3050188 (Published)

Redactable Blockchain in Decentralized Setting, by MA, Jinhua; XU, Shengmin; NING, Jianting; HUANG, Xinyi; DENG, Robert H. (2022). *IEEE Transactions on Information Forensics and Security, 17* 1227-1242. https://doi.org/10.1109/TIFS.2022.3156808 (Published)

Authenticated Data Redaction With Accountability and Transparency, by MA, Jinhua; HUANG, Xinyi; MU, Yi; DENG, Robert H.. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (1), 149-160. https://doi.org/10.1109/TDSC.2020.2998135 (Published)

ShieldFL: Mitigating Model Poisoning Attacks in Privacy-Preserving Federated Learning, by MA, ZR; MA, JF; MIAO, YB; LI, YJ; DENG, Robert H. (2022). *IEEE Transactions on Information Forensics and Security, 17* 1639-1654. (Published)

Lightweight and Expressive Fine-Grained Access Control for Healthcare Internet-of-Things, by XU, Shengmin; LI, Yingjiu; DENG, Robert H; ZHANG, Yinghui; LUO, Xiangyang; LIU, Ximeng. (2022). *IEEE Transactions on Cloud Computing, 10* (1), 474-490. https://doi.org/10.1109/TCC.2019.2936481 (Published)

Ranked keyword search over encrypted cloud data through machine learning method, by MIAO, Yinbin; ZHENG, Wei; JIA, Xiaohua; LIU, Ximeng; CHOO, Kim-Kwang Raymond; DENG, Robert H.. (2022). *IEEE Transactions on Services Computing, 16* (1), 1-12. https://doi.org/10.1109/TSC.2021.3140098 (Advance Online)

DistPreserv: Maintaining user distribution for privacy-preserving Location-Based Services, by REN, Yanbing; LI, Xinghua; MIAO, Yinbin; DENG, Robert H.; WENG, Jian; MA, Siqi; MA, Jianfeng. (2022). *IEEE Transactions on Mobile Computing, 22* (6), 1-15. https://doi.org/10.1109/TMC.2022.3141398 (Advance Online)

LinkBreaker: Breaking the Backdoor-Trigger Link in DNNs via Neurons Consistency Check, by CHEN, Zhenzhu; WANG, Shang; FU, Anmin; GAO, Yansong; YU, Shui; DENG, Robert H. (2022). *IEEE Transactions on Information Forensics and Security, 17* 2000-2014. https://doi.org/10.1109/TIFS.2022.3175616 (Published)

Secure Cloud Data Deduplication with Efficient Re-Encryption, by YUAN, Haoran; CHEN, Xiaofeng; LI, Jin; JIANG, Tao; WANG, Jianfeng; DENG, Robert H. (2022). *IEEE Transactions on Services Computing, 15* (1), 442-456. https://doi.org/10.1109/TSC.2019.2948007 (Published)

Privacy-Preserving Threshold-Based Image Retrieval in Cloud-Assisted Internet of Things, by SONG, Lin; MIAO, Yinbin; WENG, Jian; CHOO, Kim-Kwang Raymond; LIU, Ximeng; DENG, Robert H.. (2022). *IEEE Internet of Things Journal, 9* (15), 1-13. https://doi.org/10.1109/JIOT.2022.3142933 (Advance Online)

Fast and Secure Location-Based Services in Smart Cities on Outsourced Data, by WANG, Xiangyu; MA, Jianfeng; MIAO, Yinbin; LIU, Ximeng; ZHU, Dan; DENG, Robert H.. (2021). *IEEE Internet of Things Journal, 8* (24), 17639-17654. https://doi.org/10.1109/JIOT.2021.3081821 (Published)

PRICE: Privacy and Reliability-Aware Real-Time Incentive System for Crowdsensing, by ZHAO, Bowen; LIU, Ximeng; CHEN, Wei-Neng; LIANG, Wei; ZHANG, Xinglin; DENG, Robert H.. (2021). *IEEE Internet of Things Journal, 8* (24), 17584-17595. https://doi.org/10.1109/JIOT.2021.3081596 (Published)

ObliComm: Towards Building an Efficient Oblivious Communication System, by WU, Pengfei; DENG, Robert H.; SHEN, Qingni; LIU, Ximeng; LI, Qi; WU, Zhonghai. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (5), 2331-2348. (Published)

Server-Aided Bilateral Access Control for Secure Data Sharing With Dynamic User Groups, by XU, Shengmin; NING, Jianting; HUANG, Xinyi; ZHOU, Jianying; DENG, Robert H.. (2021). *IEEE Transactions on Information Forensics and Security, 16* 4746-4761. (Published)

Secure and verifiable outsourced data dimension reduction on dynamic data, by CHEN, Zhenzhu; FU, Anmin; DENG, Robert H.; LIU, Ximeng; YANG, Yang; ZHANG, Yinghui. (2021). *Information Sciences, 573* 182-193. (Published)

PriScore: Blockchain-Based Self-Tallying Election System Supporting Score Voting, by YANG, Yang; GUAN, Zhangshuang; WAN, Zhiguo; WENG, Jian; PANG, HweeHwa; DENG, Robert H.. (2021). *IEEE Transactions on Information Forensics and Security, 16* 4705-4720. (Published)

Outsourcing Service Fair Payment Based on Blockchain and Its Applications in Cloud Computing, by ZHANG, Yinghui; DENG, Robert H.; LIU, Ximeng; ZHENG, Dong. (2021). *IEEE Transactions on Services Computing, 14* (4), 1152-1166. https://doi.org/10.1109/TSC.2018.2864191 (Published)

K-Time Modifiable and Epoch-Based Redactable Blockchain, by XU, Shengmin; NING, Jianting; MA, Jinhua; HUANG, Xinyi; DENG, Robert H.. (2021). *IEEE Transactions on Information Forensics and Security, 16* 4507-4520. (Published)

Optimized Verifiable Fine-Grained Keyword Search in Dynamic Multi-Owner Settings, by MIAO, Yibin; DENG, Robert H.; CHOO, DENG, Robert H.; LIU, Ximeng; NING, Jianting; LI, Hongwei. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (4), 1804-1820. https://doi.org/10.1109/TDSC.2019.2940573 (Published)

Designing Leakage-Resilient Password Entry on Head-Mounted Smart Wearable Glass Devices, by LI, Yan; CHENG, Yao; MENG, Wenzhi; LI, Yingjiu; DENG, Robert H.. (2021). *IEEE Transactions on Information Forensics and Security, 16* 307-321. https://doi.org/10.1109/TIFS.2020.3013212 (Published)

Privacy-Preserving Proof of Storage for the Pay-As-You-Go Business Model, by WU, Tong; YANG, Guomin; MU, Yi; GUO, Fuchun; DENG, Robert H.. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (2), 563-575. https://doi.org/10.1109/TDSC.2019.2931193 (Published)

Privacy-Preserving Attribute-Based Keyword Search in Shared Multi-owner Setting, by MIAO, Yibin; LIU, Ximeng; CHOO, Kim-Kwang Raymond; DENG, Robert H.; LI, Jjguo; LI, Hongwei; MA, Jianfeng. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (3), 1-15. https://doi.org/10.1109/TDSC.2019.2897675 (Published)

Lattice-based remote user authentication from reusable fuzzy signature, by TIAN, Yangguang; LI, Yingjiu; DENG, Robert H.; SENGUPTA, Binanda; YANG, Guomin
. (2021). *Journal of Computer Security, 29* (3), 273-298. (Published)

Robust and Universal Seamless Handover Authentication in 5G HetNets, by ZHANG, Yinghui; DENG, Robert H.; BERTINO, Elisa; ZHENG, Dong. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (2), 858-874. (Published)

Looking Back! Using Early Versions of Android Apps as Attack Vectors, by ZHANG, Yue; WENG, Jian; WNEG, Jia-Si; HOU, Lin; YANG, Anjia; LI, Ming; XIANG, Yang; DENG, Robert H.. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (2), 652-666. https://doi.org/10.1109/TDSC.2019.2914202 (Published)

Secure Collaborative Deep Learning Against GAN Attacks in the Internet of Things, by CHEN, Zhenzhu; FU, Anmin; ZHANG, Yinghui; LIU, Zhe; ZENG, Fanjian; DENG, Robert H.. (2021). *IEEE Internet of Things Journal, 8* (7), 5839-5849. https://doi.org/10.1109/JIOT.2020.3033171 (Published)

Investigating the Adoption of Hybrid Encrypted Cloud Data Deduplication With Game Theory, by LIANG, Xueqin; YAN, Zheng; DENG, Robert H.; ZHENG, Qinghu. (2021). *IEEE Transactions on Parallel and Distributed Systems, 32* (3), 587-600. https://doi.org/10.1109/TPDS.2020.3028685 (Published)

Proxy-Free Privacy-Preserving Task Matching with Efficient Revocation in Crowdsourcing, by SHU, Jiangang; YANG, Kan; JIA, Xiaohua; LIU, Ximeng; WANG, Cong; DENG, Robert H.. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (1), 117-130. (Published)

Lightning-fast and privacy-preserving outsourced computation in the cloud, by LIU, Ximeng; DENG, Robert H.; WU, Pengfei; YANG, Yang. (2020). *Cybersecurity, 3* (1), 1-21. https://doi.org/10.1186/s42400-020-00057-3 (Published)

A Secure Flexible and Tampering-Resistant Data Sharing System for Vehicular Social Networks, by SUN, Jianfei; XIONG, Hu; ZHANG, Shufan; LIU, Ximeng; YUAN, Jiaming; DENG, Robert H.. (2020). *IEEE Transactions on Vehicular Technology, 69* (11), 12938-12950. https://doi.org/10.1109/TVT.2020.3015916

(Published)

VPSL: Verifiable Privacy-Preserving Data Search for Cloud-Assisted Internet of Things, by TONG, Qing; MIAO, Yinbin; LIU, Ximeng; CHOO, Kim-Kwang Raymond; DENG, Robert H.; LI, Hongwei. (2022). *IEEE Transactions on Cloud Computing, 10* (4), 1-13. https://doi.org/10.1109/TCC.2020.3031209 (Advance Online)

Attribute-based Encryption for Cloud Computing Access Control: A Survey, by ZHANG, Yinghui; DENG, Robert H.; XU, Shengmin; SUN, Jianfei; LI, Qi; ZHENG, Dong. (2020). *ACM Computing Surveys, 53* (4), 1-41. https://doi.org/10.1145/3398036 (Published)

Privacy-Preserving Outsourced Calculation Toolkit in the Cloud, by LIU, Ximeng; DENG, Robert H.; CHOO, Kim-Kwang Raymond; YANG, Yang; PANG, Hwee Hwa. (2020). *IEEE Transactions on Dependable and Secure Computing, 17* (5), 898-911. https://doi.org/10.1109/TDSC.2018.2816656 (Published)

Lightweight and Privacy-Aware Fine-Grained Access Control for IoT-Oriented Smart Health, by SUN, Jianfei; XIONG, Hu; LIU, Ximeng; ZHANG, Yinghui; NIE, Xuyun; DENG, Robert H.. (2020). *IEEE Internet of Things Journal, 7* (7), 6566-6575. https://doi.org/10.1109/JIOT.2020.2974257 (Published)

Match in My Way: Fine-Grained Bilateral Access Control for Secure Cloud-Fog Computing, by XU, Shengmin; NING, Jianting; LI, Yingjiu; ZHANG, Yinghui; XU, Guowen; HUANG, Xinyi; DENG, Robert. (2022). *IEEE Transactions on Dependable and Secure Computing, 19* (2), 1064-1077. https://doi.org/10.1109/TDSC.2020.3001557 (Published)

A new framework for privacy-preserving biometric-based remote user authentication, by TIAN, Yangguang; LI, Yingjiu; DENG, Robert H.; LI, Nan; WU, Pengfei; LIU, Anyi. (2020). *Journal of Computer Security, 28* (4), 469-498. https://doi.org/10.3233/JCS-191336 (Published)

An Extended Framework of Privacy-Preserving Computation With Flexible Access Control, by DING, Wenxiu; HU, Rui;, YAN, Zheng; QIAN, Xinren; DENG, Robert H; YANG, Laurence T.; DONG, Mianxiong. (2020). *IEEE Transactions on Network and Service Management, 17* (2), 918-930. https://doi.org/10.1109/TNSM.2019.2952462 (Published)

Editing-Enabled Signatures: A New Tool for Editing Authenticated Data, by SENGUPTA, Binanda, LI, Yingjiu; TIAN, Yangguang; DENG, Robert H.. (2020). *IEEE Internet of Things Journal, 7* (6), 4997-5007. https://doi.org/10.1109/JIOT.2020.2972741 (Published)

Secure server-aided data sharing clique with attestation, by WANG, Yujue; PANG, Hwee Hwa; DENG, Robert H.; DING, Yong; WU, Qianhong; QIN, Bo; FAN, Kefeng. (2020). *Information Sciences, 522* 80-98. https://doi.org/10.1016/j.ins.2020.02.064 (Published)

Flexible Wildcard Searchable Encryption System, by YANG, Yang; LIU, Ximeng; DENG, Robert H.; WENG, Jian. (2020). *IEEE Transactions on Services Computing, 13* (3), 464-477. https://doi.org/10.1109/TSC.2017.2714669 (Published)

Key regeneration-free ciphertext-policy attribute-based encryption and its application, by CUI, Hui; DENG, Robert H.; QIN, Baodong; WENG, Jian. (2020). *Information Sciences, 517* 217-229. https://doi.org/10.1016/j.ins.2019.12.025 (Published)

Privacy-Preserving Outsourced Support Vector Machine Design for Secure Drug Discovery, by LIU, Ximeng; DENG, Robert H.; CHOO, Kim-Kwang Raymond, YANG, Yang. (2020). *IEEE Transactions on Cloud Computing, 8* (2), 610-622. https://doi.org/10.1109/TCC.2018.2799219 (Published)

A New Construction for Linkable Secret Handshake, by TIAN, Yangguang; LI, Yingjiu; DENG, Robert H.; LI, Nan; YANG, Guomin; YANG, Zheng. (2020). *Computer Journal, 63* (4), 536-548. https://doi.org/10.1093/comjnl/bxz095 (Published)

Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Public Cloud, by DENG, Hua; QIN, Zheng; WU, Qianhong; GUAN, Zhenyu; DENG, Robert H.; WANG, Yujue; ZHOU, Yunya. (2020). *IEEE Transactions on Information Forensics and Security, 15* 3168-3180. https://doi.org/10.1109/TIFS.2020.2985532 (Published)

Game theoretical study on client-controlled cloud data deduplication, by LIANG, Xueqin; YAN, Zheng; DENG, Robert H.. (2020). *Computers and Security, 91* 1-14. https://doi.org/10.1016/j.cose.2020.101730 (Published)

Multi-User Multi-Keyword Rank Search Over Encrypted Data in Arbitrary Language, by YANG, Yang; LIU,

Ximeng; DENG, Robert H. (2020). *IEEE Transactions on Dependable and Secure Computing, 17* (2), 320-334. https://doi.org/10.1109/TDSC.2017.2787588 (Published)

Privacy-Preserving Data Processing with Flexible Access Control, by DING, Wenxiu; YAN, Zheng; DENG, Robert H.. (2020). *IEEE Transactions on Dependable and Secure Computing, 17* (2), 363-376. https://doi.org/10.1109/TDSC.2017.2786247 (Published)

Privacy-preserving Network Path Validation, by SENGUPTA, Binanda; LI, Yingjiu; BU, Kai; DENG, Robert H.. (2020). *ACM Transactions on Internet Technology, 20* (1), 5:1-5:27. https://doi.org/10.1145/3372046 (Published)

Server-aided revocable attribute-based encryption for cloud computing services, by CUI, Hui; YUEN, Tsz Hon; DENG, Robert H.; WANG, Guilin. (2020). *Concurrency and Computation: Practice and Experience, 32* (14), 1-16. https://doi.org/10.1002/cpe.5680 (Published)

Lightweight sharable and traceable secure mobile health system, by YANG, Yang; LIU, Ximeng; DENG, Robert H.; LI, Yingjiu. (2020). *IEEE Transactions on Dependable and Secure Computing, 17* (1), 78-91. https://doi.org/10.1109/TDSC.2017.2729556 (Published)

Toward Highly Secure Yet Efficient KNN Classification Scheme on Outsourced Cloud Data, by LIU, Lin; SU, Jinshu; LIU, Ximeng; CHEN, Rongmao; HUANG, Kai; DENG, Robert H.; WANG, Xiaofeng. (2019). *IEEE Internet of Things Journal, 6* (6), 9841-9852. https://doi.org/10.1109/JIOT.2019.2932444 (Published)

Data Security Issues in Deep Learning: Attacks, Countermeasures, and Opportunities, by XU, Guowen; LI, Hongwei; REN, Hao; YANG, Kan; DENG, Robert H.. (2019). *IEEE Communications Magazine, 57* (11), 116-122. https://doi.org/10.1109/MCOM.001.1900091 (Published)

Secure Online/Offline Data Sharing Framework for Cloud-Assisted Industrial Internet of Things, by MIAO, Yinbin; TONG, Qiuyun; CHOO, Kim-Kwang Raymond; LIU, Ximeng; DENG, Robert H; LI, Hongwei. (2019). *IEEE Internet of Things Journal, 6* (5), 8681-8691. https://doi.org/10.1109/JIOT.2019.2923068 (Published)

Efficient and Robust Certificateless Signature for Data Crowdsensing in Cloud-Assisted Industrial IoT, by ZHANG, Yinghui; DENG, Robert H.; ZHENG, Dong; LI, Jin; WU, Pengfei; CAO, Jin. (2019). *IEEE Transactions on Industrial Informatics, 15* (9), 5099-5108. https://doi.org/10.1109/TII.2019.2894108 (Published)

Multi-Authority Attribute-Based Keyword Search over Encrypted Cloud Data, by MIAO, Yibin; DENG, Robert H.; LIU, Ximeng; CHOO, Kim-Kwang Raymond.; WU, Hongjun; LI, Hongwei. (2021). *IEEE Transactions on Dependable and Secure Computing, 18* (4), 1-14. https://doi.org/10.1109/TDSC.2019.2935044 (Published)

Securing messaging services through efficient signcryption with designated equality test, by WANG, Yujue; PANG, Hwee Hwa; DENG, Robert H.; DING, Yong; WU, Qianhong; QIN, Bo. (2019). *Information Sciences, 490* 145-165. https://doi.org/10.1016/j.ins.2019.03.039 (Published)

Hybrid Keyword-Field Search With Efficient Key Management for Industrial Internet of Things, by MIAO, Yinbin; LIU, Ximeng; DENG, Robert H.; WU, Hongjun; LI, Hongwei; LI, Jiguo; WU. Dapeng. (2019). *IEEE Transactions on Industrial Informatics, 15* (6), 3206-3217. https://doi.org/10.1109/TII.2018.2877146 (Published)

Collusion attacks and fair time-locked deposits for fast-payment transactions in Bitcoin, by YU, Xingjie; THANG, Michael Shiwen; LI, Yingjiu.; DENG, Robert H.. (2019). *Journal of Computer Security, 27* (3), 375-403. https://doi.org/10.3233/JCS-191274 (Published)

CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing, by LI, Ming; WENG, Jian; YANG, Anjia; LU, Wei; ZHANG, Yue; HOU, Lin; LIU, Jia-Nan; XIANG, Yang; DENG, Robert H.. (2019). *IEEE Transactions on Parallel and Distributed Systems, 30* (6), 1251-1266. https://doi.org/10.1109/TPDS.2018.2881735 (Published)

A blockchain-based location privacy-preserving crowdsensing system, by YANG, Mengmeng; ZHU, Tianqing; LIANG, Kaitai; ZHOU, Wanlei; DENG, Robert H.. (2019). *Future Generation Computer Systems: The International Journal of eScience, 94* 408-418. https://doi.org/10.1016/j.future.2018.11.046 (Published)

Fair and Dynamic Data Sharing Framework in Cloud-Assisted Internet of Everything, by MIAO, Yinbin; LIU, Ximeng; CHOO, Kim-Kwang Raymond; DENG, Robert H.; WU, Hongjun; LI, Hongwei. (2019). *IEEE Internet of Things Journal, 6* (4), 7201-7212. https://doi.org/10.1109/JIOT.2019.2915123 (Published)

Attribute-Based Storage Supporting Secure Deduplication of Encrypted Data in Cloud, by CUI, Hui; DENG, Robert H.; LI, Yingjiu; WU, Guowei. (2019). *IEEE Transactions on Big Data, 5* (3), 330-342. https://doi.org/10.1109/TBDATA.2017.2656120 (Published)

MicroBTC: Efficient, Flexible and Fair Micropayment for Bitcoin Using Hash Chains, by WAN, Zhiguo; DENG, Robert H.; LEE, David; LI, Ying. (2019). *Journal of Computer Science and Technology, 34* (2), 403-415. https://doi.org/10.1007/s11390-019-1916-x (Published)

An Attribute-Based Framework for Secure Communications in Vehicular Ad Hoc Networks, by CUI, Hui; DENG, Robert H.; WANG, Guilin. (2019). *IEEE/ACM Transactions on Networking, 27* (2), 721-733. https://doi.org/10.1109/TNET.2019.2894625 (Published)

Situation-Aware Authenticated Video Broadcasting Over Train-Trackside WiFi Networks, by WU, Yongdong; YE, Dengpan; WEI, Zhuo; WANG, Qian; TAN, William; DENG, Robert Huijie. (2019). *IEEE Internet of Things Journal, 6* (2), 1617-1627. https://doi.org/10.1109/JIOT.2018.2859185 (Published)

SybSub: Privacy-Preserving Expressive Task Subscription With Sybil Detection in Crowdsourcing, by SHU, Jiangang; LIU, Ximeng; YANG, Kan; ZHANG, Yinghui; JIA, Xiaohua; DENG, Robert H.. (2019). *IEEE Internet of Things Journal, 6* (2), 3003-3013. https://doi.org/10.1109/JIOT.2018.2877780 (Published)

Privacy-Preserving Reinforcement Learning Design for Patient-Centric Dynamic Treatment Regimes, by LIU, Ximeng; DENG, Robert H.; CHOO, Kim-Kwang Raymond; YANG, Yang. (2021). *IEEE Transactions on Emerging Topics in Computing, 9* (1), 1-15. https://doi.org/10.1109/TETC.2019.2896325 (Published)

When Human cognitive modeling meets PINs: User-independent inter-keystroke timing attacks, by LIU, Ximing; LI, Yingjiu; DENG, Robert H.; CHANG, Bing; LI, Shujun. (2019). *Computers and Security, 80* 90-107. https://doi.org/10.1016/j.cose.2018.09.003 (Published)

Secure smart health with privacy-aware aggregate authentication and access control in Internet of Things, by ZHANG, Yinghui; DENG, Robert H.; HAN, Gang; ZHENG, Dong. (2018). *Journal of Network and Computer Applications, 123* 89-100. https://doi.org/10.1016/j.jnca.2018.09.005 (Published)

VPSearch: Achieving Verifiability for Privacy-Preserving Multi-Keyword Search over Encrypted Cloud Data, by WAN, Zhiguo; DENG, Robert H.. (2018). *IEEE Transactions on Dependable and Secure Computing, 15* (6), 1083-1095. https://doi.org/10.1109/TDSC.2016.2635128 (Published)

Resonance Attacks on Load Frequency Control of Smart Grids, by WU, Yongdong; WEI, Zhuo; WENG, Jian; LI, Xin; DENG, Robert H.. (2018). *IEEE Transactions on Smart Grid, 9* (5), 4490-4502. https://doi.org/10.1109/TSG.2017.2661307 (Published)

Blockchain based efficient and robust fair payment for outsourcing services in cloud computing, by ZHANG, Yinghui; DENG, Robert H.; LIU, Ximeng; ZHENG, Dong. (2018). *Information Sciences, 462* 262-277. https://doi.org/10.1016/j.ins.2018.06.018 (Published)

Making a good thing better: enhancing password/PIN-based user authentication with smartwatch, by CHANG, Bing; LI, Yingjiu; WANG, Qiongxiao; ZHU, Wen-Tao; DENG, Robert H.. (2018). *Cybersecurity, 1* (1), 1-13. https://doi.org/10.1186/s42400-018-0009-4 (Published)

Server-Aided Attribute-Based Signature With Revocation for Resource-Constrained Industrial-Internet-of-Things Devices, by CUI, Hui; DENG, Robert H.; LIU, Joseph K.; YI, Xun; LI, Yingjiu. (2018). *IEEE Transactions on Industrial Informatics, 14* (8), 3724-3732. https://doi.org/10.1109/TII.2018.2813304 (Published)

Anonymous Privacy-Preserving Task Matching in Crowdsourcing, by SHU, Jiangang; LIU, Ximeng; JIA, Xiaohua; YANG, Kan; DENG, Robert H.. (2018). *IEEE Internet of Things Journal, 5* (4), 3068-3078. https://doi.org/10.1109/JIOT.2018.2830784 (Published)

Lightweight Break-Glass Access Control System for Healthcare internet-of-Things, by YANG, Yang; LIU, Ximeng; DENG, Robert H.. (2018). *IEEE Transactions on Industrial Informatics, 14* (8), 3610-3617. https://doi.org/10.1109/TII.2017.2751640 (Published)

TKSE: Trustworthy Keyword Search Over Encrypted Data With Two-Side Verifiability via Blockchain, by ZHANG, Yinghui; DENG, Robert H.; SHU, Jiangang; YANG, Kan; ZHENG, Dong. (2018). *IEEE Access, 6* 31077-31087. https://doi.org/10.1109/ACCESS.2018.2844400 (Published)

Verifiably encrypted cascade-instantiable blank signatures to secure progressive decision management, by WANG, Yujue; PANG, Hwee Hwa; DENG, Robert H.. (2018). *International Journal of Information*

*Security, 17* (3), 347-363. https://doi.org/10.1007/s10207-017-0372-2 (Published)

Position Manipulation Attacks to Balise-Based Train Automatic Stop Control, by WU, Yongdong; WEI, Zhuo; WENG, Jian; DENG, Robert H.. (2018). *IEEE Transactions on Vehicular Technology, 67* (6), 5287-5301. https://doi.org/10.1109/TVT.2018.2802444 (Published)

Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control, by ZHANG, Yinghui; ZHENG, Dong; DENG, Robert H.. (2018). *IEEE Internet of Things Journal, 5* (3), 2130-2145. https://doi.org/10.1109/JIOT.2018.2825289 (Published)

Expressive query over outsourced encrypted data, by YANG, Yang; LIU, Ximeng; DENG, Robert H.. (2018). *Information Sciences, 442* 33-53. https://doi.org/10.1016/j.ins.2018.02.017 (Published)

Efficient and Expressive Keyword Search Over Encrypted Data in Cloud, by CUI, Hui; WAN, Zhiguo; DENG, Robert H.; WANG, Guilin; LI, Yingjiu. (2018). *IEEE Transactions on Dependable and Secure Computing, 15* (3), 409-422. https://doi.org/10.1109/TDSC.2016.2599883 (Published)

Empirical Study of Face Authentication Systems Under OSNFD Attacks, by LI, Yan; LI, Yingjiu; XU, Ke; YAN, Qiang; DENG, Robert H.. (2018). *IEEE Transactions on Dependable and Secure Computing, 15* (2), 231-245. https://doi.org/10.1109/TDSC.2016.2550459 (Published)

An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, revisited, by CUI, Hui; DENG, Robert H.; LAI, Junzuo; YI, Xun; NEPAL, Surya. (2018). *Computer Networks, 133* 157-165. https://doi.org/10.1016/j.comnet.2018.01.034 (Published)

Secure Fine-Grained Access Control and Data Sharing for Dynamic Groups in the Cloud, by XU, Shengmin; YANG, Guomin; MU, Yi; DENG, Robert H.. (2018). *IEEE Transactions on Information Forensics and Security, 13* (8), 2101-2103. https://doi.org/10.1109/TIFS.2018.2810065 (Published)

Attribute-based cloud storage with secure provenance over encrypted data, by CUI, Hui; DENG, Robert H.; LI, Yingjiu. (2018). *Future Generation Computer Systems: The International Journal of eScience, 79* (2), 461-472. https://doi.org/10.1016/j.future.2017.10.010 (Published)

Hybrid privacy-preserving clinical decision support system in fog-cloud computing, by LIU, Ximeng; DENG, Robert H.; YANG, Yang; TRAN, Hieu N.; ZHONG, Shangping. (2018). *Future Generation Computer Systems: The International Journal of eScience, 78* (2), 825-837. https://doi.org/10.1016/j.future.2017.03.018 (Published)

Efficient and Privacy-Preserving Outsourced Calculation of Rational Numbers, by LIU, Ximeng; CHOO, Kim-Kwang Raymond; DENG, Robert H.; LU, Rongxing; WENG, Jian. (2018). *IEEE Transactions on Dependable and Secure Computing, 15* (1), 27-39. https://doi.org/10.1109/TDSC.2016.2536601 (Published)

TinyVisor: An extensible secure framework on android platforms, by SHEN, Dong; LI, Zhoujun; SU, Xiaojing; MA, Jinxin; DENG, Robert H.. (2018). *Computers and Security, 72* 145-162. https://doi.org/10.1016/j.cose.2017.09.006 (Published)

CCA Secure encryption supporting authorized equality test on ciphertexts in standard model and its applications, by WANG, Yujue; PANG, Hwee Hwa; TRAN, Ngoc Hieu; DENG, Robert H.. (2017). *Information Sciences, 414* 289-305. https://doi.org/10.1016/j.ins.2017.06.008 (Published)

An Efficient Privacy-Preserving Outsourced Computation over Public Data, by LIU, Ximeng; QIN, Baodong; DENG, Robert; LI, Yingjiu. (2017). *IEEE Transactions on Services Computing, 10* (5), 756-770. https://doi.org/10.1109/TSC.2015.2511008 (Published)

Related-key secure key encapsulation from extended computational bilinear Diffie-Hellman, by QIN, Brandon; LIU, Shengli; SUN, Shifeng; DENG, Robert H.; GU, Dawu. (2017). *Information Sciences, 406* 1-11. https://doi.org/10.1016/j.ins.2017.04.018 (Published)

HIBS-KSharing: Hierarchical Identity-Based Signature Key Sharing for Automotive, by WEI, Zhuo; YANG, Yanjiang; WU, Yongdong; WENG, Jian; DENG, Robert H.. (2017). *IEEE Access, 5* 16314-16323. https://doi.org/10.1109/ACCESS.2017.2737957 (Published)

A Secure, Usable, and Transparent Middleware for Permission Managers on Android, by WANG, Daibin; YAO, Haixia; LI, Yingjiu; JIN, Hai; ZOU, Deqing; DENG, Robert H.. (2017). *IEEE Transactions on Dependable and Secure Computing, 14* (4), 350-362. https://doi.org/10.1109/TDSC.2015.2479613 (Published)

Encrypted data processing with Homomorphic Re-Encryption, by DING, Wenxiu; YAN, Zheng; DENG, Robert H.. (2017). *Information Sciences, 409* 35-55. https://doi.org/10.1016/j.ins.2017.05.004 (Published)

A study on a feasible no-root approach on Android, by CHENG, Yao; LI, Yingjiu; DENG, Robert; YING, Lingyun; HE, Wei. (2017). *Journal of Computer Security, 25* (3), 231-253. https://doi.org/10.3233/JCS-16866 (Published)

Identity-Based Data Outsourcing With Comprehensive Auditing in Clouds, by WANG, Yujue; WU, Qianhong; QIN, Bo; SHI, Wenchang; DENG, Robert H.; HU, Jiankun. (2017). *IEEE Transactions on Information Forensics and Security, 12* (4), 940-952. https://doi.org/10.1109/TIFS.2016.2646913 (Published)

Vulnerabilities, Attacks, and Countermeasures in Balise-Based Train Control Systems, by WU, Yongdong; WENG, Jian; TANG, Zhe; LI, Xin; DENG, Robert H.. (2017). *IEEE Transactions on Intelligent Transportation Systems, 18* (4), 814-823. https://doi.org/10.1109/TITS.2016.2590579 (Published)

Universally Composable RFID Mutual Authentication, by SU, Chunhua; SANTOSO, Bagus; LI, Yingjiu; DENG, Robert; HUANG, Xinyi. (2017). *IEEE Transactions on Dependable and Secure Computing, 14* (1), 83-94. http://doi.org/10.1109/TDSC.2015.2434376 (Published)

Ciphertext-policy attribute-based encryption with partially hidden access structure and its application to privacy-preserving electronic medical record system in cloud environment, by LIU, Lixian; LAI, Junzuo; DENG, Robert H.; LI, Yingjiu. (2016). *Security and Communication Networks, 9* (18), 4897-4913. https://doi.org/10.1002/sec.1663 (Published)

A Privacy-Preserving Outsourced Functional Computation Framework Across Large-Scale Multiple Encrypted Domains, by LIU, Ximeng; QIN, Baodong; DENG, Robert H.; LU, Rongxing; MA, Jianfeng. (2016). *IEEE Transactions on Computers, 65* (12), 3567-3579. https://doi.org/10.1109/TC.2016.2543220 (Published)

On the security of two identity-based conditional proxy re-encryption schemes, by HE, Kai; WENG, Jian; DENG, Robert H.; LIU, Joseph K.. (2016). *Theoretical Computer Science, 652* 18-27. http://doi.org/10.1016/j.tcs.2016.08.023 (Published)

An Efficient Privacy-Preserving Outsourced Calculation Toolkit With Multiple Keys, by LIU, Ximeng; DENG, Robert H.; CHOO, Kim-Kwang Raymond; WENG, Jian. (2016). *IEEE Transactions on Information Forensics and Security, 11* (11), 2401-2414. https://doi.org/10.1109/TIFS.2016.2573770 (Published)

An Efficient Privacy-Preserving Outsourced Calculation Toolkit With Multiple Keys, by LIU, Ximeng; DENG, Robert H.; CHOO, Raymond; WENG, Jian. (2016). *IEEE Transactions on Information Forensics and Security, 11* (11), 2401-2414. http://doi.org/10.1109/TIFS.2016.2573770 (Published)

Privacy-Preserving Outsourced Calculation on Floating Point Numbers, by LIU, Ximeng; DENG, Robert H.; DING, Wenxiu; LU, Rongxing, QIN, Baodong. (2016). *IEEE Transactions on Information Forensics and Security, 11* (11), 2513-2527. https://doi.org/10.1109/TIFS.2016.2585121 (Published)

Escrow free attribute-based signature with self-revealability, by CUI, Hui; WANG, Guilin; DENG, Robert H.; QIN, Baodong. (2016). *Information Sciences, 367* 660-672. http://doi.org/10.1016/j.ins.2016.07.010 (Published)

Trustworthy Authentication on Scalable Surveillance Video with Background Model Support, by WEI, Zhuo; YAN, Zheng; WU, Yongdong; DENG, Robert H.. (2016). *ACM Transactions on Multimedia Computing, Communications and Applications, 12* (4), 1-20. http://doi.org/10.1145/2978573 (Published)

Revocable and Decentralized Attribute-Based Encryption, by CUI, Hui; DENG, Robert H.. (2016). *Computer Journal, 59* (8), 1220-1235. https://doi.org/10.1093/comjnl/bxw007 (Published)

A Survey on Future Internet Security Architectures, by DING, Wenxiu; YAN, Zheng; DENG, Robert H.. (2016). *IEEE Access, 4* 4374-4393. https://doi.org/10.1109/ACCESS.2016.2596705 (Published)

Adaptable key-policy attribute-based encryption with time interval, by MA, Siqi; LAI, Junzuo; DENG, Robert H.; DING, Xuhua. (2017). *Soft Computing, 21* (20), 6191-6200. https://doi.org/10.1007/s00500-016-2177-z (Published)

Deduplication on encrypted big data in cloud, by YAN, Zheng; DING, Wenxiu; YU, Xixun; ZHU, Haiqi; DENG, Robert H.. (2016). *IEEE Transactions on Big Data, 2* (2), 138-150. https://doi.org/10.1109/TBDATA.2016.2587659 (Published)

ICCDetector: ICC-Based Malware Detection on Android, by XU, Ke; LI, Yingjiu; DENG, Robert H.. (2016). *IEEE Transactions on Information Forensics and Security, 11* (6), 1252-1264. https://doi.org/10.1109/TIFS.2016.2523912 (Published)

A note on the security of KHL scheme, by WENG, Jian; ZHAO, Yunlei; DENG, Robert H.; LIU, Shengli; YANG, Yanjiang; SAKURAI, Kouichi. (2015). *Theoretical Computer Science, 602* 1-6. https://doi.org/10.1016/j.tcs.2015.07.051 (Published)

On robust image spam filtering via comprehensive visual modeling, by SHEN, Jialie; DENG, Robert H.; CHENG, Zhiyong; NIE, Liqiang; YAN, Shuicheng. (2015). *Pattern Recognition, 48* (10), 3227-3238. https://doi.org/10.1016/j.patcog.2015.02.027 (Published)

Attribute-Based Encryption With Efficient Verifiable Outsourced Decryption, by QIN, Baodong; DENG, Robert H.; LIU, Shengli; MA, Siqi. (2015). *IEEE Transactions on Information Forensics and Security, 10* (7), 1384-1393. https://doi.org/10.1109/TIFS.2015.2410137 (Published)

Efficient revocable certificateless encryption against decryption key exposure, by SUN, Yinxia; ZHANG, Futai; SHEN, Limin; DENG, Robert H.. (2015). *IET Information Security, 9* (3), 158-166. http://dx.doi.org/10.1049/iet-ifs.2014.0145 (Published)

Privacy leakage analysis in online social networks, by LI, Yan; LI Yingjiu; YAN, Qiang; DENG, Robert H.. (2015). *Computers and Security, 49* 239-254. https://doi.org/10.1016/j.cose.2014.10.012 (Published)

Leakage-resilient password entry: Challenges, design, and evaluation, by YAN, Qiang; HAN, Jin; LI, Yingjiu; ZHOU, Jianying; DENG, Robert H.. (2015). *Computers and Security, 48* 196-211. https://doi.org/10.1016/j.cose.2014.10.008 (Published)

Software Puzzle: A Countermeasure to Resource-Inflated Denial-of-Service Attacks, by WU, Yongdong; ZHAO, Zhigang; FENG, Bao; DENG, Robert H.. (2015). *IEEE Transactions on Information Forensics and Security, 10* (1), 168-177. https://doi.org/10.1109/TIFS.2014.2366293 (Published)

Unforgeability of an improved certificateless signature scheme in the standard model, by GUAN, Chaowen; WENG, Jian; DENG, Robert H.; CHEN, Minrong; ZHOU, Dehua. (2014). *IET Information Security, 8* (5), 273-276. http://dx.doi.org/10.1049/iet-ifs.2013.0062 (Published)

Towards semantically secure outsourcing of association rule mining on categorical data, by LAI, Junzuo; LI, Yingjiu; DENG, Robert H.; WENG, Jian; GUAN, Chaowen; YAN, Qiang. (2014). *Information Sciences, 267* 267-286. https://doi.org/10.1016/j.ins.2014.01.040 (Published)

Technique for authenticating H.264/SVC and its performance evaluation over wireless mobile networks, by ZHAO, Yifan; LO, Swee Won; DENG, Robert H.; DING, Xuhua. (2014). *Journal of Computer and System Sciences, 80* (3), 520-532. https://doi.org/10.1016/j.jcss.2013.06.008 (Published)

A Hybrid Scheme for Authenticating Scalable Video Codestreams, by WEI, Zhuo; WU, Yongdong; DENG, Robert H.; DING, Xuhua. (2014). *IEEE Transactions on Information Forensics and Security, 9* (4), 543-553. https://doi.org/10.1109/TIFS.2014.2301916 (Published)

Efficient block-based transparent encryption for H.264/SVC bitstreams, by DENG, Robert H.; DING, Xuhua; WU, Yongdong; WEI, Zhuo. (2014). *Multimedia Systems, 20* (2), 165-178. http://dx.doi.org/10.1007/s00530-013-0326-0 (Published)

Efficient authentication and access control of scalable multimedia streams over packet-lossy networks, by DENG, Robert H.; DING, Xuhua; LO, Swee Won. (2014). *Security and Communication Networks, 7* (3), 611-625. https://doi.org/10.1002/sec.762 (Published)

Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage, by CHU, Cheng-Kang; CHOW, Sherman M. M; TZENG, Wen-Guey; ZHOU, Jiangying; DENG, Robert H.. (2014). *IEEE Transactions on Parallel and Distributed Systems, 25* (2), 468-477. http://doi.org/10.1109/TPDS.2013.112 (Published)

A Collusion-Resistant Conditional Access System for Flexible-Pay-Per-Channel Pay-TV Broadcasting, by WAN, Zhiguo; LIU, June; ZHANG, Rui; DENG, Robert H.. (2013). *IEEE Transactions on Multimedia, 15* (6), 1353-1364. https://doi.org/10.1109/TMM.2013.2250493 (Published)

DriverGuard: Virtualization-Based Fine-Grained Protection on I/O Flows, by CHENG, Yueqiang; DING, Xuhua; DENG, Robert H.. (2013). *ACM Transactions on Information and System Security, 16* (2), 6-30. http://dx.doi.org/10.1145/2505123 (Published)

Attribute-Based Encryption With Verifiable Outsourced Decryption, by LAI, Junzuo; DENG, Robert H.; GUAN, Chaowen; WENG, Jian. (2013). *IEEE Transactions on Information Forensics and Security, 8* (8), 1343-1354. https://doi.org/10.1109/TIFS.2013.2271848 (Published)

Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks, by WU, Yongdong; WEI, Zhuo; DENG, Robert H.. (2013). *IEEE Transactions on Multimedia, 15* (4), 778-788. http://doi.org/10.1109/TMM.2013.2238910 (Published)

A secure platform for information sharing in EPCglobal network, by SHI, Jie; LI, Yingjiu; DENG, Robert H.; HE, Wei; LEE, Eng Wah. (2013). *International Journal of RFID Security and Cryptography, 2* (1/4), 107-118. (Published)

Enhanced authentication for commercial video services, by HUANG, Xinyi; CHU, Cheng-Kang; SUN, Hung-Min; ZHOU, Jianying; DENG, Robert H.. (2012). *Security and Communication Networks, 5* (11), 1248-1259. http://dx.doi.org/10.1002/sec.620 (Published)

A scalable and format-compliant encryption scheme for H.264/SVC bitstreams, by Wei, Zhuo; Wu, Yongdong; DING, Xuhua; DENG, Robert H.. (2012). *Signal Processing: Image Communication, 27* (9), 1011-1024. http://dx.doi.org/10.1016/j.image.2012.06.005 (Published)

Scalable content authentication in H.264/SVC videos using perceptual hashing based on Dempster-Shafer theory, by YE, Dengpan; ZHUO, Wei; DING, Xuhua; DENG, Robert H.. (2012). *International Journal of Computational Intelligence Systems, 5* (5), 953-963. (Published)

A secure and efficient discovery service system in EPCglobal network, by SHI, Jie; LI, Yingjiu; DENG, Robert H.. (2012). *Computers and Security, 31* (8), 870-885. https://doi.org/10.1016/j.cose.2012.08.005 (Published)

TruBeRepec: a trust-behavior-based reputation and recommender system for mobile applications, by YAN, Zheng; ZHANG, Peng; DENG, Robert H.. (2012). *Personal and Ubiquitous Computing, 16* (5), 485-506. http://dx.doi.org/10.1007/s00779-011-0420-2 (Published)

HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing, by WAN, Zhiguo; LIU, Jun'e; DENG, Robert H.. (2012). *IEEE Transactions on Information Forensics and Security, 7* (2), 743-754. https://doi.org/10.1109/TIFS.2011.2172209 (Published)

Detecting node replication attacks in mobile sensor networks: theory and approaches, by ZHU, Wen Tao; Zhou, Jianying; DENG, Robert H.; Bao, Feng. (2012). *Security and Communication Networks, 5* (5), 496-507. http://dx.doi.org/10.1002/sec.338 (Published)

Detecting node replication attacks in wireless sensor networks: A survey, by ZHU, Wen Tao; Zhou, Jianying; DENG, Robert H.; Bao, Feng. (2012). *Journal of Network and Computer Applications, 35* (3), 1022-1034. http://dx.doi.org/10.1016/j.jnca.2012.01.002 (Published)

A Survey on Privacy Frameworks for RFID Authentication, by SU, Chunhua; LI, Yingjiu; ZHAO, Yunlei; DENG, Robert H.; ZHAO, Yiming; ZHOU, Jianying. (2012). *IEICE Transactions on Information and Systems, E95D* (1), 2-11. https://doi.org/10.1587/transinf.E95.D.2 (Published)

Anti-tracking in RFID discovery service for dynamic supply chain systems, by YAN, Qiang; LI, Yingjiu; DENG, Robert H.. (2012). *International Journal of RFID Security and Cryptography, 1* (1), 25-35. http://infonomics-society.org/IJRFIDSC/IJRFIDSC_Paper 4.pdf (Published)

On Two RFID Privacy Notions and Their Relations, by LI, Yingjiu; DENG, Robert H.; LAI, Junzuo; MA, Changshe. (2011). *ACM Transactions on Information and System Security, 14* (4), 1-23. https://doi.org/10.1145/2043628.2043631 (Published)

A zero-knowledge based framework for RFID privacy, by DENG, Robert H.; LI, Yingjiu; YUNG, Moti; ZHAO, Yunlei. (2011). *Journal of Computer Security, 19* (6), 1109-1146. https://doi.org/10.3233/JCS-2011-0440 (Published)

Improved Ordinary Measure and Image Entropy Theory based intelligent Copy Detection Method, by YE, Dengpan; MA, Longfei; WANG, Lina; DENG, Robert H.. (2011). *International Journal of Computational Intelligence Systems, 4* (5), 777-787. https://doi.org/10.1080/18756891.2011.9727829 (Published)

A Generic Framework for Three-Factor Authentication: Preserving Security and Privacy in Distributed Systems, by HUANG, Xinyi; XIANG, Yang; CHONKA, Ashley; ZHOU, Jianying; DENG, Robert H.. (2011). *IEEE*

*Transactions on Parallel and Distributed Systems, 22* (8), 1390-1397. https://doi.org/10.1109/TPDS.2010.206 (Published)

General construction of chameleon all-but-one trapdoor functions, by LIU, Shengli; LAI, Junzuo; DENG, Robert H.. (2011). *Journal of Internet Services and Information Security, 1* (2/3), 74-88. http://isyou.info/jisis/vol1/no23/jisis-2011-vol1-no23-06.pdf (Published)

Secure localization with attack detection in wireless sensor networks, by ZHU, Wentao; XIANG, Yang; ZHOU, Jianying; DENG, Robert H.; FENG, Bao. (2011). *International Journal of Information Security, 10* (3), 155-171. http://dx.doi.org/10.1007/s10207-011-0127-4 (Published)

Preserving Transparency and Accountability in Optimistic Fair Exchange of Digital Signatures, by HUANG, Xinyi; MU, Yi; SUSILO, Willy; ZHOU, Jianying; DENG, Robert H.. (2011). *IEEE Transactions on Information Forensics and Security, 6* (2), 489-512. https://doi.org/10.1109/TIFS.2011.2109952 (Published)

Cryptanalysis of a certificateless signcryption scheme in the standard model, by WENG, Jian; YAO, Guoxiang; DENG, Robert H.; CHEN, Min-Rong; LI, Xianxue. (2011). *Information Sciences, 181* (3), 661-667. https://doi.org/10.1016/j.ins.2010.09.037 (Published)

Database Access Pattern Protection Without Full-Shuffles, by DING, Xuhua; YANG, Yanjiang; DENG, Robert H.. (2011). *IEEE Transactions on Information Forensics and Security, 6* (1), 189-201. https://doi.org/10.1109/TIFS.2010.2101062 (Published)

Secure mobile agents with controlled resources, by ZHANG, Qi; Mu, Yi; ZHANG, Minjie; DENG, Robert H.. (2011). *Concurrency and Computation: Practice and Experience, 23* (12), 1348-1366. http://dx.doi.org/10.1002/cpe.1618 (Published)

Chosen-ciphertext secure bidirectional proxy re-encryption schemes without pairings, by WENG, Jian; DENG, Robert H.; LIU, Shengli; CHEN, Kefei. (2010). *Information Sciences, 180* (24), 5077-5089. http://dx.doi.org/10.1016/j.ins.2010.08.017 (Published)

A new hardware-assisted PIR with O(n) shuffle cost, by DING, Xuhua; YANG, Yanjiang; DENG, Robert H.; WANG, Shuhong. (2010). *International Journal of Information Security, 9* (4), 237-252. https://doi.org/10.1007/s10207-010-0105-2 (Published)

New Constructions for Identity-Based Unidirectional Proxy Re-Encryption, by LAI, Junzuo; ZHU, Wen Tao; DENG, Robert H.; LIU, Shengli; KOU, Weidong. (2010). *Journal of Computer Science and Technology, 25* (4), 793-806. https://doi.org/10.1007/s11390-010-9366-5 (Published)

Time-Bound Hierarchical Key Assignment: An Overview, by ZHU, Wen Tao; DENG, Robert H.; Zhou, Jianying; Bao, Feng. (2010). *IEICE Transactions on Information and Systems, E93D* (5), 1044-1052. https://doi.org/10.1587/transinf.E93.D.1044 (Published)

Cryptanalysis of a Hierarchical Identity-Based Encryption Scheme, by Weng, Jian; CHEN, Min-Rong; CHEN, Kefei; DENG, Robert H.. (2010). *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E93A* (4), 854-856. http://dx.doi.org/10.1587/transfun.E93.A.854 (Published)

Shifting Inference Control to User Side: Architecture and Protocol, by YANG, Yanjiang; LI, Yingjiu; DENG, Robert H.; BAO, Feng. (2010). *IEEE Transactions on Dependable and Secure Computing, 7* (2), 189-202. https://doi.org/10.1109/TDSC.2008.70 (Published)

CCA-secure unidirectional proxy re-encryption in the adaptive corruption model without random oracles, by WENG, Jian; CHEN, Minrong; YANG, Yanjiang; DENG, Robert H.; CHEN, Kefei. (2010). *Science in China Series F: Information Sciences, 53* (3), 593-606. https://doi.org/10.1007/s11432-010-0047-3 (Published)

A Multi-Key Pirate Decoder Against Traitor Tracing Schemes, by Wu, Yongdong; DENG, Robert H.. (2010). *Journal of Computer Science and Technology, 25* (2), 362-374. http://dx.doi.org/10.1007/s11390-010-9329-x (Published)

Efficient discrete logarithm based multi-signature scheme in the plain public key model, by MA, Changshe; Weng, Jian; LI, Yingjiu; DENG, Robert H.. (2010). *Designs, Codes and Cryptography, 54* (2), 121-133. http://dx.doi.org/10.1007/s10623-009-9313-z (Published)

TeleOph: A Secure Real-Time Teleophthalmology System, by WU, Yongdong; WEI, Zhou; YAO, Haixia; ZHAO, Zhigang; NGOH, Lek Heng; DENG, Robert H.; YU, Shengsheng. (2010). *IEEE Transactions on Information Technology in Biomedicine, 14* (5), 1259-1266. https://doi.org/10.1109/TITB.2010.2058124 (Published)

Achieving high security and efficiency in RFID-tagged supply chains, by CAI, Shaoying; LI, Yingjiu; LI, Tieyan; DENG, Robert H.; YAO, Haixia. (2010). *International Journal of Applied Cryptography, 2* (1), 3-12. https://doi.org/10.1504/IJACT.2010.033794 (Published)

On the potential of limitation-oriented malware detection and prevention techniques on mobile phones, by YAN, Qiang; DENG, Robert H.; LI, Yingjiu; LI, Tieyan. (2010). *International Journal of Security and Its Applications, 4* (1), 21-30. http://www.sersc.org/journals/IJSIA/vol4_no1_2010/3.pdf (Published)

A Study of Content Authentication in Proxy-Enabled Multimedia Delivery Systems: Model, Techniques, and Applications, by DENG, Robert H.; YANG, Yanjiang. (2009). *ACM Transactions on Multimedia Computing, Communications and Applications, 5* (4), 28:1-20. https://doi.org/10.1145/1596990.1596992 (Published)

Privacy-preserving rental services using one-show anonymous credentials, by YANG, Yanjiang; DENG, Robert H.; Bao, Feng. (2009). *Security and Communication Networks, 2* (6), 531-545. http://dx.doi.org/10.1002/sec.97 (Published)

Better security enforcement in trusted computing enabled heterogeneous wireless sensor networks, by YANG, Yanjiang; Zhou, Jianying; DENG, Robert H.; Bao, Feng. (2011). *Security and Communication Networks, 4* (1), 11-22. http://dx.doi.org/10.1002/sec.179 (Published)

Multiuser private queries over encrypted databases, by YANG, Yanjiang; Bao, Feng; DING, Xuhua; DENG, Robert H.. (2009). *International Journal of Applied Cryptography, 1* (4), 309-319. http://dx.doi.org/10.1504/IJACT.2009.028029 (Published)

nPAKE<SUP>+</SUP>: A Tree-Based Group Password-Authenticated Key Exchange Protocol Using Different Passwords, by WAN, Zhiguo; DENG, Robert H.; BAO, Feng; PRENEEL, Bart; GU, Ming. (2009). *Journal of Computer Science and Technology, 24* (1), 138-151. http://dx.doi.org/10.1007/s11390-009-9207-6 (Published)

A Secure and Synthesis Tele-Ophthalmology System, by Wei, Zhuo; Wu, Yongdong; DENG, Robert H.; YU, Shengsheng; YAO, Haixia; ZHAO, Zhigang; NGOH, Lek Heng; LIM, Tock Han; POH, Eugenie. (2008). *Telemedicine and e-Health, 14* (8), 833-845. http://dx.doi.org/10.1089/tmj.2008.0086 (Published)

The security and improvement of an ultra-lightweight RFID authentication protocol, by LI, Tieyan; DENG, Robert H.; WANG, Guilin. (2008). *Security and Communication Networks, 1* (2), 135-146. http://dx.doi.org/10.1002/sec.8 (Published)

Security analysis on a family of ultra-lightweight RFID authentication protocols, by LI, Tieyan; WANG, Guilin; DENG, Robert H.. (2008). *Journal of Software, 3* (3), 1-10. http://dx.doi.org/10.4304/jsw.3.3.1-10 (Published)

Flexible access control to JPEG 2000 image code-streams, by WU, Yongdong; MA, Di; DENG, Robert H.. (2007). *IEEE Transactions on Multimedia, 9* (6), 1314-1324. https://doi.org/10.1109/TMM.2007.902865 (Published)

Techniques for hiding mobile node's location movement information in Mobile IP, by DENG, Robert H.; QIU, Ying; ZHOU, Jianying; BAO, Feng. (2007). *China Communications, 4* (1), 85-94. (Published)

Access control protocols with two-layer architecture for wireless networks, by WAN, Zhiguo; DENG, Robert H.; BAO, Feng; ANANDA, Akkihebbal L.. (2007). *Computer Networks, 51* (3), 655-670. https://doi.org/10.1016/j.comnet.2006.05.009 (Published)

A secure extension of the Kwak-Moon group signcryption scheme, by Kwak, D.; Moon, S. J.; WANG, Guilin; DENG, Robert H.. (2006). *Computers and Security, 25* (6), 435-444. http://dx.doi.org/10.1016/j.cose.2006.05.006 (Published)

Three architectures for trusted data dissemination in edge computing, by GOH, Shen-Tat; PANG, Hwee Hwa; DENG, Robert H.; BAO, Feng. (2006). *Data & Knowledge Engineering, 58* (3), 381-409. https://doi.org/10.1016/j.datak.2005.05.003 (Published)

A novel privacy preserving authentication and access control scheme for pervasive computing environments, by REN, Kui; LOU, Wenjing; KIM, Kwangjo; DENG, Robert H.. (2006). *IEEE Transactions on Vehicular Technology, 55* (4), 1373-1384. http://dx.doi.org/10.1109/TVT.2006.877704 (Published)

Security analysis on a conference scheme for mobile communications, by WAN, Zhiguo; BAO, Feng; DENG, Robert H.; ANANDA, A. L.. (2006). *IEEE Transactions on Wireless Communications, 5* (6), 1238-1240.

https://doi.org/10.1109/TWC.2006.1638641 (Published)

A practical password-based two-server authentication and key exchange system, by YANG, Yanjiang; DENG, Robert H.; BAO, Feng. (2006). *IEEE Transactions on Dependable and Secure Computing, 3* (2), 105-114. https://doi.org/10.1109/TDSC.2006.16 (Published)

Scalable authentication of MPEG-4 streams, by WU, Yongdong; DENG, Robert H.. (2006). *IEEE Transactions on Multimedia, 8* (1), 152-161. https://doi.org/10.1109/TMM.2005.861283 (Published)

Routing optimization security in mobile IPv6, by Ren, Kui; Lou, Wenjing; Zeng, Kai; Bao, Feng; Zhou, Jianying; DENG, Robert H.. (2006). *Computer Networks, 50* (13), 2401-2419. http://dx.doi.org/10.1016/j.comnet.2005.09.019 (Published)

Minimizing TTP's involvement in signature validation, by ZHOU, Jianying; BAO, Feng; DENG, Robert H.. (2006). *International Journal of Information Security, 5* (1), 37-47. http://doi.org/10.1007/s10207-005-0072-1 (Published)

New efficient MDS array codes for RAID -: Part II:: Rabin-like codes for tolerating multiple (≥ 4) disk failures, by FENG, Gui-Liang; DENG, Robert H.; BAO, Feng. (2005). *IEEE Transactions on Computers, 54* (12), 1473-1483. https://doi.org/10.1109/TC.2005.200 (Published)

Tailored reversible watermarking schemes for authentication of electronic clinical atlas, by BAO, Feng; DENG, Robert H.; OOI, Beng-Chin; YANG, Yanjiang. (2005). *IEEE Transactions on Information Technology in Biomedicine, 9* (4), 554-563. https://doi.org/10.1109/TITB.2005.855556 (Published)

Scalable trusted online dissemination of JPEG2000 images, by DENG, Robert H.; MA, Di; Shao, Weizhong; Wu, Yongdong. (2005). *Multimedia Systems, 11* (1), 60-67. http://dx.doi.org/10.1007/s00530-005-0190-7 (Published)

New efficient MDS array codes for RAID part I: Reed-Solomon-like codes for tolerating three disk failures, by FENG, Gui-Liang; DENG, Robert H.; BAO, Feng; SHEN, Jia-Chen. (2005). *IEEE Transactions on Computers, 54* (9), 1071-1080. https://doi.org/10.1109/TC.2005.150 (Published)

Efficient and robust key management for large mobile ad hoc networks, by ZHU, Bo; BAO, Feng; DENG, Robert H.; KANKANHALLI, Mohan S.; WANG, Guilin. (2005). *Computer Networks, 48* (4), 657-682. http://dx.doi.org/10.1016/j.comnet.2004.11.023 (Published)

Protocols that hide user's preferences in electronic transactions, by BAO, Feng; DENG, Robert H.. (2005). *Computer Networks, 48* (4), 503-515. http://dx.doi.org/10.1016/j.comnet.2004.10.010 (Published)

Security of an Ill-posed operator for image authentication, by WU, Yongdong; DENG, Robert H.. (2005). *IEEE Transactions on Circuits and Systems for Video Technology, 15* (1), 161-163. https://doi.org/10.1109/TCSVT.2004.839978 (Published)

New efficient user identification and key distribution scheme providing enhanced security, by YANG, Yanjiang; WANG, Shuhong; BAO, Feng; WANG, Jie; DENG, Robert H.. (2004). *Computers and Security, 23* (8), 697-704. http://dx.doi.org/10.1016/j.cose.2004.08.005 (Published)

Comments on "A practical (t, n) threshold proxy signature scheme based on the RSA cryptosystem", by WANG, Guilin; BAO, Feng; ZHOU, Jianying; DENG, Robert H.. (2004). *IEEE Transactions on Knowledge and Data Engineering, 16* (10), 1309-1311. https://doi.org/10.1109/TKDE.2004.52 (Published)

A smart-card-enabled privacy preserving e-prescription system, by YANG, Yanjiang; HAN, Xiaoxi; BAO, Feng; DENG, Robert H.. (2004). *IEEE Transactions on Information Technology in Biomedicine, 8* (1), 47-58. http://doi.org/10.1109/TITB.2004.824731 (Published)

Highly reliable trust establishment scheme in ad hoc networks, by REN, K.; LI, Tieyan; WAN, Zhiguo; BAO, Feng; DENG, Robert H.; KIM, K.. (2004). *Computer Networks, 45* (6), 687-699. http://doi.org/10.1016/j.comnet.2004.01.008 (Published)

Content-aware authentication of motion JPEG2000 stream in lossy networks, by WU, Yongdong; DENG, Robert H.. (2003). *IEEE Transactions on Consumer Electronics, 49* (4), 792-801. https://doi.org/10.1109/TCE.2003.1261157 (Published)

Cryptanalysis of some hash functions based on block ciphers and codes, by WU, Hongjun; BAO, Feng; DENG, Robert H.. (2002). *Informatica, 26* (3), 255-258. (Published)

Multicast Internet protocol, by WANG, X. K.; DENG, Robert H.; BAO, Feng. (2000). *Computer Communications, 23* (11), 1047-1054. https://doi.org/10.1016/s0140-3664(00)00167-5 (Published)

On the validity of digital signatures, by Zhou, J.; DENG, Robert H.. (2000). *Computer Communication Review, 30* (2), 29-34. http://dx.doi.org/10.1145/505680.505684 (Published)

Capture model for mobile radio slotted ALOHA systems, by ZHOU, Huafei; DENG, Robert H.. (1998). *IEE Proceedings Communications, 145* (2), 91-97. http://dx.doi.org/10.1049/ip-com:19981839 (Published)

Integrating security in the CORBA architecture, by DENG, Robert H.; BHONSIE, Shailendra K.; WANG, Weiguo; LAZAR, Aurel A.. (1997). *Theory and Practice of Object Systems, 3* (1), 3-13. https://doi.org/10.1002/(SICI)1096-9942(1997)3:1<3::AID-TAPO2>3.0.CO;2-Y (Published)

An on-the-fly decoding technique for Reed-Solomon codes, by LEE, Yuan Xing; DENG, Robert H.; KOH, Eng Hean. (1996). *IEEE Transactions on Magnetics, 32* (5), 3962-3964. https://doi.org/10.1109/20.539231 (Published)

Type-1 hybrid ARQ scheme with time diversity for binary digital FM cellular radio, by ZHOU, Huafei; DENG, Robert H.. (1996). *IEE Proceedings Communications, 143* (1), 29-36. http://dx.doi.org/10.1049/ip-com:19960373 (Published)

Practical Protocols for Certified Electronic Mail, by DENG, Robert H.; Gong, L.; Lazar, A. A.; WANG, W.. (1996). *Journal of Network and Systems Management, 4* (3), 279-297. http://dx.doi.org/10.1007/bf02139147 (Published)

A type I hybrid ARQ system with adaptive code rates, by DENG, Robert H.; LIN, Michael L.. (1995). *IEEE Transactions on Communications, 43* 733-737. https://doi.org/10.1109/26.380101 (Published)

(D,K/I) CONSTRAINED PARTIAL-RESPONSE MAXIMUM-LIKELIHOOD CODES, by LI, Y. X.; Subrahmanyam, J.; DENG, Robert H.. (1995). *International Journal of Electronics, 78* (1), 19-24. http://dx.doi.org/10.1080/00207219508926136 (Published)

HYBRID ARQ SCHEMES EMPLOYING CODED MODULATION AND SEQUENCE COMBINING, by DENG, Robert H.. (1994). *IEEE Transactions on Communications, 42* (6), 2239-2245. http://dx.doi.org/10.1109/26.293675 (Published)

PERFORMANCE OF COMBINED DIVERSITY RECEPTION AND CONVOLUTIONAL CODING FOR QDPSK LAND MOBILE RADIO, by ZHOU, Huafei; DENG, Robert H.; TJHUNG, Tjeng T.. (1994). *IEEE Transactions on Vehicular Technology, 43* (3), 499-508. https://doi.org/10.1109/25.312797 (Published)

EXACT AND APPROXIMATE MODELS TO OBTAIN AVERAGE THROUGHPUT OF THE FDDI MAC PROTOCOL .2. ASYMMETRIC SYSTEMS, by LIM, K. S.; DENG, Robert H.; Ranai, K.. (1994). *Computer Communications, 17* (4), 251-256. http://dx.doi.org/10.1016/0140-3664(94)90079-5 (Published)

SIMULATING A MULTIMEDIA FDDI BACKBONE NETWORK, by Ranai, K.; LIM, K. S.; DENG, Robert H.. (1994). *Computer Journal, 37* (3), 188-198. http://dx.doi.org/10.1093/comjnl/37.3.188 (Published)

EXACT AND APPROXIMATE MODELS TO OBTAIN AVERAGE THROUGHPUT OF THE FDDI MAC PROTOCOL .2. ASYMMETRIC SYSTEMS, by LIM, K. S.; DENG, Robert H.; Ranai, K.. (1994). *Computer Communications, 17* (4), 83-93. http://dx.doi.org/10.1016/S0140-3664(05)80013-1 (Published)

ON THE EQUIVALENCE OF MCELIECE AND NIEDERREITER PUBLIC-KEY CRYPTOSYSTEMS, by LI, Y. X.; DENG, Robert H.; WANG, X. M.. (1994). *IEEE Transactions on Information Theory, 40* (1), 271-273. https://doi.org/10.1109/18.272496 (Published)

A probabilistic approach to fault diagnosis in linear lightwave networks, by DENG, Robert H.; LAZAR, A. A.; WANG, W.. (1993). *IEEE Journal on Selected Areas in Communications, 11* (9), 1438-1448. https://doi.org/10.1109/49.257935 (Published)

AN ADAPTIVE CODING SCHEME WITH CODE COMBINING FOR MOBILE RADIO SYSTEMS, by DENG, Robert H.; ZHOU, Huafei. (1993). *IEEE Transactions on Vehicular Technology, 42* (4), 469-476. https://doi.org/10.1109/25.260765 (Published)

DC-FREE ERROR-CORRECTING CONVOLUTIONAL-CODES, by DENG, Robert H.; LI, Y. X.; HERRO, M. A.. (1994). *Electronics Letters, 30* (21), 1910-1911. https://doi.org/10.1049/el:19931271 (Published)

NEW PARITY RETRANSMISSION SYSTEM USING PRODUCT CODES, by DENG, Robert H.. (1993). *IEE*

*Proceedings Communications, 140* (5), 351-356. http://dx.doi.org/10.1049/ip-i-2.1993.0052 (Published)

HYBRID ARQ SCHEMES FOR POINT-TO-MULTIPOINT COMMUNICATION OVER NONSTATIONARY BROADCAST CHANNELS, by DENG, Robert H.. (1993). *IEEE Transactions on Communications, 41* (9), 1379-1387. https://doi.org/10.1109/26.237857 (Published)

LAN-BASED MEDICAL VISUALIZATION COMMUNICATION-SYSTEM, by DENG, Robert H.; Shu, R.. (1993). *Computer Communications, 16* (8), 518-525. http://dx.doi.org/10.1016/0140-3664(93)90067-3 (Published)

PERFORMANCE ANALYSIS OF 2 BRIDGED CSMA CD NETWORKS, by KO, Chi Chung; WANG, W. C.; DU, Jiangling; DENG, Robert H.; LYE, K. M.. (1993). *Computer Communications, 16* (8), 501-510. https://doi.org/10.1016/0140-3664(93)90065-Z (Published)

PERFORMANCE OF A TOKEN-PASSING SYSTEM WITH BATCH ARRIVALS AND ITS APPLICATION TO FILE TRANSFERS, by DENG, Robert H.; ZHANG, Xuanyu; HUANG, Kuan Tase. (1993). *Computer Communications, 16* (7), 422-431. https://doi.org/10.1016/0140-3664(93)90103-Y (Published)

PERFORMANCE ANALYSIS OF INTERCONNECTED LANS WITH SERVER CLIENT CONFIGURATION, by DU, Jiangling; DENG, Robert H.; KO, Chi Chung. (1993). *Computer Networks and ISDN Systems, 25* (12), 1321-1333. https://doi.org/10.1016/0169-7552(93)90022-v (Published)

EFFECTS OF STATION BUFFER CAPACITY ON TOKEN RING NETWORK PERFORMANCE, by DENG, Robert H.; Chiew, W. C. L.. (1993). *Computer Communications, 16* (6), 366-375. http://dx.doi.org/10.1016/0140-3664(93)90118-C (Published)

PERFORMANCE OF CONVOLUTIONAL CODING WITH SYMBOL ERASURE FOR QPSK FREQUENCY-SELECTIVE FADING CHANNELS, by ZHOU, Huafei; DENG, Robert H.. (1993). *IEICE Transactions on Communications, E76B* (2), 139-147. http://ci.nii.ac.jp/naid/110003216921 (Published)

NEW SELECTION DIVERSITY RECEPTION SCHEME EFFECTIVE FOR BOTH FREQUENCY-FLAT AND SELECTIVE FADING CHANNELS, by ZHOU, Huafei; DENG, Robert H.; YOSHIDA, S.. (1992). *Electronics Letters, 28* (25), 2297-2298. https://doi.org/10.1049/el:19921478 (Published)

HYBRID ARQ SCHEME USING TCM AND CODE COMBINING, by DENG, Robert H.. (1991). *Electronics Letters, 27* (10), 866-868. http://dx.doi.org/10.1049/el:19910542 (Published)

END-TO-END PERFORMANCE OF INTERCONNECTED LANS, by BERG, Brigitte; DENG, Robert H.. (1991). *Computer Communications, 14* (2), 105-112. http://dx.doi.org/10.1016/0140-3664(91)90040-8 (Published)

GATEWAY DESIGN FOR LAN INTERCONNECTION VIA ISDN, by ZHANG, Xian-Yu; DENG, Robert H.. (1990). *Computer Networks and ISDN Systems, 19* (1), 43-51. https://doi.org/10.1016/0169-7552(90)90117-b (Published)

TRELLIS-CODED MULTIDIMENSIONAL PHASE MODULATION, by PIETROBON, Steven S.; DENG, Robert H.; LAFANECHERE, Alain; UNGERBOECK, Gottfried; COSTELLO, Daniel J.. (1990). *IEEE Transactions on Information Theory, 36* (1), 63-89. https://doi.org/10.1109/18.50375 (Published)

HIGH-RATE CONCATENATED CODING SYSTEMS USING BANDWIDTH EFFICIENT TRELLIS INNER CODES, by DENG, Robert H.; COSTELLO, Daniel J., JR.. (1989). *IEEE Transactions on Communications, 37* (5), 1091-1096. https://doi.org/10.1109/26.24593 (Published)

HIGH-RATE CONCATENATED CODING SYSTEMS USING MULTIDIMENSIONAL BANDWIDTH-EFFICIENT TRELLIS INNER CODES, by DENG, Robert H.; COSTELLO, Daniel J. Jr.. (1989). *IEEE Transactions on Communications, 37* (10), 1091-1096. https://doi.org/10.1109/26.41155 (Published)

NEW POINT-TO-MULTIPOINT COMMUNICATION PROTOCOLS, by DENG, Robert H.; ZHANG, X. Y.; THAM, Y. K.. (1989). *IEE Proceedings Communications, 136* (4), 312-316. http://dx.doi.org/10.1049/ip-i-2.1989.0044 (Published)

PARITY RETRANSMISSION HYBRID ARQ USING RATE 1/2 CONVOLUTIONAL-CODES ON A NONSTATIONARY CHANNEL, by LUGAND, L. R.; COSTELLO, D. J.; DENG, Robert H.. (1989). *IEEE Transactions on Communications, 37* (7), 755-765. https://doi.org/10.1109/26.31168 (Published)

DC-FREE COSET CODES, by DENG, Robert H.; HERRO, M. A.. (1988). *IEEE Transactions on Information Theory, 34* (4), 786-792. https://doi.org/10.1109/18.9775 (Published)

DECODING OF DBEC-TBED REED-SOLOMON CODES, by DENG, Robert H.; COSTELLO, Daniel J. Jr.. (1987).

*IEEE Transactions on Computers, 36* (11), 1359-1363. https://doi.org/10.1109/TC.1987.5009476 (Published)

RELIABILITY AND THROUGHPUT ANALYSIS OF A CONCATENATED CODING SCHEME, by DENG, Robert H.; COSTELLO, Daniel J.. (1987). *IEEE Transactions on Communications, 35* (7), 698-705. https://doi.org/10.1109/TCOM.1987.1096850 (Published)

Journal Articles [Non-Refereed]

Driving Cybersecurity Policy Insights From Information on the Internet, by WANG, Qiu-Hong; MILLER, Steven M.; DENG, Robert H.. (2020). *IEEE Security and Privacy, 18* (6), 42-50. https://doi.org/10.1109/MSEC.2020.3000765 (Published)

Editorials

Guest Editorial: 5G-Enabled Intelligent Application for Distributed Industrial Internet-of-Thing System, by LIU, Ximeng; DENG, Robert H.; MIAO, Yibin; Vasilakos, Athanasios V.. (2022). *IEEE Transactions on Industrial Informatics, 18* (4), 2807-2810. https://doi.org/10.1109/TII.2021.3123971 (Published)

Data Fusion for Trust Evaluation, by YAN, Zheng; ZHENG, Qinghua; YANG, Laurence T.; DENG Robert H.. (2021). *Information Fusion, 76* 187-188. (Published)

Cryptography and Data Security in Cloud Computing, by YAN, Zheng; DENG, Robert H.; VARADHARAJAN, Vijay. (2017). *Information Sciences, 387* 53-55. http://doi.org/10.1016/j.ins.2016.12.034 (Published)

Editorial: Trust Management for Multimedia Big Data, by YAN, Zheng; LIU, Jun; DENG, Robert H.; HERRERA, Francisco. (2016). *ACM Transactions on Multimedia Computing, Communications and Applications, 12* (4), 1-2. https://doi.org/10.1145/2978431 (Published)

Security and privacy of electronic health information systems, by BERTINO, Elisa; DENG, Robert H.; HUANG, Xinyi; ZHOU, Jianying. (2015). *International Journal of Information Security, 14* (6), 485-486. http://dx.doi.org/10.1007/s10207-015-0303-z (Published)

Editorial: special issue on ubiquitous electronic commerce systems, by DENG, Robert H.; VEIJALAINEN, Jari; LIAN, Shiguo; KANELLOPOULOS, Dimitris. (2011). *Electronic Commerce Research, 11* (1), 1-4. https://doi.org/10.1007/s10660-010-9071-z (Published)

Books (Refereed)

*Leakage resilient password systems* by LI, Yingjiu; YAN, Qiang; DENG, Robert H.. (2015). SpringerBriefs in Computer Science, Cham: Springer. https://doi.org/10.1007/978-3-319-17503-4 (Published)

*RFID security and privacy* by LI, Yingjiu; DENG, Robert H.; BERTINO, Elisa. (2013). San Rafael, CA: Morgan & Claypool. https://doi.org/10.2200/S00550ED1V01Y201311SPT007 (Published)

Book Chapters

Trust Management in Mobile Platforms, by YAN, Zheng; CHENG, Yanxiao; YAN, Ping; DENG, Robert H.. (2018). In LEE, David Kuo Chuen; DENG, Robert (Ed.), *Handbook of Blockchain, Digital Finance, and Inclusion* (pp. 83-113) Elsevier Inc.. http://doi.org/10.1016/B978-0-12-812282-2.00005-X (Published)

When seeing is not believing: Defeating MFF-based attacks by liveness detection for face authentication on mobile platform, by LI, Yan; YAN, Qiang; LI, Yingjiu; DENG, Robert H.. (2016). In Weizhi Meng, Xiapu Luo, Steven Furnell, Jianying Zhou (Ed.), *Protecting mobile networks and devices: Challenges and solutions* (pp. 29-48) Taylor & Francis Group. https://worldcat.org/isbn/9781498735834 (Published)

Malware Protection on RFID-Enabled Supply Chain Management Systems in the EPCglobal Network, by YAN, Qiang; LI, Yingjiu; DENG, Robert H.. (2013). In A. Miri (Ed.), *Advanced security and privacy for RFID technologies* (pp. 153-175) Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-4666-3685-9 (Published)

Dynamic secure cloud storage with provenance, by CHOW, Sherman; CHU, Cheng-Kang; HUANG, Xinyi; ZHOU, Jianying; DENG, Robert H.. (2012). In D. Naccache (Ed.), *Cryptography and security: From theory to*

*applications* (pp. 442-464) Berlin: Springer. https://doi.org/10.1007/978-3-642-28368-0_28 (Published)

Remote platform attestation: The testimony for trust management, by DING, Xuhua; Gu, LIANG; DENG, Robert H.; Xie, Bing; MEI, Hong. (2010). *Trust modelling and management in digital environments: From social concept to system development* (pp. 1-19) Hershey, PA: IGI Global. https://doi.org/10.4018/978-1-61520-682-7.ch001 (Published)

Enforcing security in mobile networks: Challenges and solutions, by DENG, Robert H.; BAO, Feng; QIU, Ying; ZHOU, Jianying. (2006). In R. Shorey, A. L. Ananda, M. C. Chan and W. T. Ooi (Ed.), *Mobile, wireless and sensor networks: Technology, applications and future directions* Hoboken, NJ: Wiley. https://doi.org/10.1002/0471755591.ch14 (Published)

Securing JPEG2000 code-streams, by DENG, Robert H.; Wu, Yongdong; MA, Di. (2005). In D.T. Lee, S. Shieh & D. Tygar (Ed.), *Security in the 21st Century* (pp. 229-253) Berlin: Springer. https://doi.org/10.1007/0-387-24006-3_13 (Published)

Security analysis of three oblivious transfer protocols, by YAO, Gang; BAO, Feng; DENG, Robert H.. (2004). In K. Feng, H. Niederreiter, and C. Xing (Ed.), *Coding, cryptography and combinatorics* (pp. 387-396) Boston: Birkhauser Verlag. https://doi.org/10.1007/978-3-0348-7865-4_27 (Published)

Edited Books

*Handbook of blockchain, digital finance, and inclusion: Cryptocurrency, FinTech, InsurTech, and regulation,* edited by LEE, David; DENG, Robert H.. (2018). San Diego, CA: Academic Press. https://doi.org/10.1016/C2015-0-04334-9 (Published)

Book Reviews

Web Security Sourcebook: A Complete Guide to Web Security Threats and Solutions [book review], by DENG, Robert H.. (1999). *Computer Communications, 22* (6), 591-591 http://dx.doi.org/10.1016/S0140-3664(99)00069-9 (Published)

Bring Network Security out of the Closet, by DENG, Robert H.. (1995). *Computer Communications, 18* (1), 55-56 http://dx.doi.org/10.1016/0140-3664(95)90074-8 (Published)

Comprehensive Token Ring Coverage (Book Review), by DENG, Robert H.. (1994). *Computer Communications, 17* (1), 75-76 http://dx.doi.org/10.1016/0140-3664(94)90022-1 (Published)

Conference Proceedings

Efficient and secure Spatial Range Query over large-scale encrypted data, by MIAO, Yinbin; XU, Chao; ZHENG, Yifeng; LIU, Ximeng; MENG, Xiangdong; DENG, Robert H.. (2023.0). *Proceedings of the 43rd IEEE International Conference on Distributed Computing Systems (ICDCS 2023), Hong Kong, China, July 18-21,* (pp. 271-281) New York, NY, USA: IEEE. https://doi.org/10.1109/ICDCS57875.2023.00055 (Published)

Communication efficient federated learning based on adaptive local differential privacy, by MIAO, Yinbin; XIE, Rongpeng; LI, Xinghua; LIU, Ximeng; MA, Zhuo; DENG, Robert H.. (2022.0). *Proceedings of the Annual Computer Security Applications Conference, Austin, Texas, 2022 December 5-9,* USA: (Published)

M-EDESE: Multi-Domain, Easily Deployable, and Efficiently Searchable Encryption, by YUAN, Jiaming; LI, Yingjiu; NING, Jianting; DENG, Robert H.. (2022.0). *Information Security Practice and Experience : 17th International Conference, ISPEC 2022, Taipei, November 23-25: Proceedings,* (pp. 606-623) Cham: Springer. https://doi.org/10.1007/978-3-031-21280-2_34 (Published)

Lightweight privacy-preserving spatial keyword query over encrypted cloud data, by YANG, Yutao; MIAO, Yinbin; CHOO, Kim-Kwang Raymond; DENG, Robert H.. (2022.0). *Proceedings of the 42nd IEEE International Conference on Distributed Computing Systems, Bologna, Italy, 2022 July 10 - 13,* (pp. 392-402) Bologna: https://doi.ieeecomputersociety.org/10.1109/ICDCS54860.2022.00045 (Published)

FREED: an efficient privacy-preserving solution for person re-identification, by ZHAO, Bowen; LI, Yingjiu; LIU, Ximeng; PANG, Hwee Hwa; Deng, Robert H.; . (2022.0). *Proceedings of the 5th IEEE Conference on Dependable and Secure Computing, Edinburgh, United Kingdom, 2022 June 22 - 24,* Edinburgh: https://doi.org/10.1109/DSC54232.2022.9888863 (Published)

LEAP: Leakage-abuse attack on efficiently deployable, efficiently searchable encryption with partially known dataset, by NING, Jianting; HUANG, Xinyi; POH, Geong Sen; YUAN, Jiaming; LI, Yingjiu; WENG, Jian; DENG, Robert H.. (2021.0). *Proceedings of the 2021 ACM Conference on Computer and Communications Security (ACM CCS 2021), Virtual Conference, November 15-19,* (pp. 2307-2320) Virtual Conference: ACM. (Published)

Revocable policy-based Chameleon hash, by XU, Shengmin; NING, Jianting; MA, Jinhua; XU, Guowen; YUAN, Jiaming; DENG, Robert H.. (2021.0). *Computer Security: ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4-8: Proceedings,* (pp. 327-347) Cham: Springer. https://doi.org/10.1007/978-3-030-88418-5_16 (Published)

When program analysis meets bytecode search: Targeted and efficient inter-procedural analysis of modern Android apps in BackDroid, by WU, Daoyuan; GAO, Debin; DENG, Robert H.; CHANG, Rocky. (2021.0). *Proceedings of the 51st IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2021),* (pp. 543-554) Online: (Published)

Expressive bilateral access control for Internet-of-Things in cloud-fog computing, by XU, Shengmin; NING, Jianting; MA, Jinhua; HUANG, Xinyi; PANG, Hwee Hwa; DENG, Robert H.. (2021.0). *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies (SACMAT 2021), Virtual Conference, June 16-18,* (pp. 143-154) Virtual Conference: ACM. (Published)

UltraPIN: Inferring PIN entries via ultrasound, by LIU; Ximing; LI, Yingjiu; DENG, Robert H.. (2021.0). *Proceedings of the ACM Asia Conference on Computer and Communications Security (ACM ASIACCS 2021),* (pp. 944-957) Online: (Published)

Efficient and verifiable proof of replication with fast fault localization, by YUAN, Haoran; CHEN, Xiaofeng; XU, Guowen; NING, Jianting; LIU, Joseph; DENG, Robert H.. (2021.0). *Proceedings of 2021 the IEEE International Conference on Computer Communications, Vancouver, May 10-13,* Virtual Conference: IEEE. (Published)

Differential training: A generic framework to reduce label noises for Android malware detection, by XU, Jiayun; LI, Yingjiu; DENG, Robert H.. (2021.0). *Proceedings of the 2021 Network and Distributed System Security Symposium (NDSS 2021),* Online: (Published)

Secure and verifiable inference in deep neural networks, by XU, Gouwen; LI, Hongwei; REN, Hao; SUN, Jianfei; XU, Shengmin; NING, Jianting; YANG, Haomiao; YANG, Kan; DENG, Robert, H.. (2020.0). *ACSAC '20: Proceedings of the 36th Annual Computer Security Applications Conference, Virtual, December 7-11,* (pp. 784-797) New York: ACM. https://doi.org/10.1145/3427228.3427232 (Published)

A deep learning framework supporting model ownership protection and traitor tracing, by XU, Guowen; LI, Hongwei; ZHANG, Yuan; LIN, Xiaodong; DENG, Robert H.; SHEN, Xuemin (Sherman). (2020.0). *2020 IEEE International Conference on Parallel and Distributed Systems 26th ICPADS: Virtual, December 2-4: Proceedings,* (pp. 438-446) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/ICPADS51040.2020.00084 (Published)

Boosting privately: Federated extreme gradient boosting for mobile crowdsensing, by LIU, Yang; MA, Zhuo; LIU, Ximeng; MA, Siqi; NEPAL, Surya; DENG, Robert H.; REN, Kui.. (2020.0). *2020 40th IEEE International Conference on Distributed Computing Systems (ICDCS): Singapore, November 29 - December 1: Proceedings,* (pp. 1-11) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/ICDCS47774.2020.00017 (Published)

Catch you if you deceive me: Verifiable and privacy-aware truth discovery in crowdsensing systems, by XU, Guowen; LI, Hongwei; XU, Shengmin; REN, Hao; ZHANG, Yinghui; SUN, Jianfei; DENG, Robert H.. (2020.0). *ASIA CCS '20: Proceedings of the 15th ACM Asia Conference on Computer and Communications Security: Virtual, Taiwan, October 5-9,* (pp. 178-192) New York: ACM. https://doi.org/10.1145/3320269.3384720 (Published)

Pine: Enabling privacy-preserving deep packet inspection on TLS with rule-hiding and fast connection establishment, by NING, Jianting; HUANG, Xinyi; POH, Geong Sen; LOH, Jia-Ch'ng; WENG, Jian; DENG, Robert H.. (2020.0). *Computer Security ESORICS 2020: Proceedings of the 25th Symposium, Guildford, United Kingdom, September 14-18,* (pp. 3-22) Cham: Springer. https://doi.org/10.1007/978-3-030-58951-6_1 (Published)

Search me in the dark: Privacy-preserving Boolean range query over encrypted spatial data, by WANG, Xiangyu; MA, Jianfeng; LIU, Ximeng; DENG, Robert H.; MIAO, Yinbin; ZHU, Dan; MA, Zhuoran. (2020.0). *2020 38th IEEE Conference on Computer Communications, INFOCOM: Toronto, Canada; July 6-9:*

*Proceedings,* (pp. 2253-2262) Piscataway, NJ: IEEE. https://doi.org/10.1109/INFOCOM41043.2020.9155505 (Published)

Understanding Android VoIP security: A system-level vulnerability assessment, by HE, De; WU, Daoyuan; DENG, Robert H.. (2020.0). *Detection of Intrusions and Malware, and Vulnerability Assessment: Proceedings of the 17th International Conference, DIMVA 2020, Lisbon, Portugal; June 24-26,* (pp. 110-131) Switzerland: Springer. https://doi.org/10.1007/978-3-030-52683-2_6 (Published)

An empirical study of SMS one-time password authentication in Android apps, by MA, Siqi; FENG, Runhan; LI, Juanru; LIU, Yang; NEPAL, Surya; BERTINO, Elisa; DENG, Robert H.; MA, Zhuo; JHA, Sanjay. (2019.0). *Proceedings of the 35th Annual Computer Security Applications Conference (ACSAC 2019),* (pp. 339-354) San Juan: ACM. https://doi.org/10.1145/3359789.3359828 (Published)

Lightweight attribute-based keyword search with policy protection for cloud-assisted IoT, by SUN, Jianfei; XIONG, Hu; DENG, Robert H.; ZHANG, Yinghui; LIU, Ximeng; CAO, Mingsheng. (2019.0). *2019 IEEE Conference on Dependable and Secure Computing 3rd DSC: Hangzhou, China, November 18-20: Proceedings,* Piscataway, NJ: IEEE. https://doi.org/10.1109/DSC47296.2019.8937708 (Published)

Random delay attack and its applications on load frequency control of power systems, by WU, Yongdong; WENG, Jian; QIU, Bo; WEI, Zhuo; QIAN, Fan; DENG, Robert H.. (2019.0). *2019 IEEE Conference on Dependable and Secure Computing 3rd DSC: Hangzhou, China, November 18-21: Proceedings,* Piscataway, NJ: IEEE. https://doi.org/10.1109/DSC47296.2019.8937611 (Published)

Finding flaws from password authentication code in Android apps, by MA, Siqi; BERTINO, Elisa; NEPAL, Surya; LI, Jianru; DIETHELM, Ostry; DENG, Robert H.; JHA, Sanjay. (2019.0). *Computer Security: ESORICS 2019: Proceedings of the European Symposium on Research in Computer Security, Luxembourg, September 15,* (pp. 619-637) Cham: Springer. https://doi.org/10.1007/978-3-030-29959-0_30 (Published)

A closer look tells more: A facial distortion based liveness detection for face authentication, by LI, Yan; WANG, Zilong; LI, Yingjiu; DENG, H. Robert; CHEN, Binbin; MENG, Weizhi; LI, Hui. (2019.0). *AsiaCCS 2019: Proceedings of the ACM Asia Conference on Information, Computer and Communications Security, Auckland, July 9-12,* (pp. 241-246) New York: ACM. https://doi.org/10.1145/3321705.3329850 (Published)

Towards understanding Android system vulnerabilities: Techniques and insights, by WU, Daoyuan; GAO, Debin; CHENG, Eric K. T.; CAO, Yichen; JIANG, Jintao; DENG, Robert H.. (2019.0). *ASIACCS 2019: Proceedings of the 14th ACM ASIA Conference on Computer and Communications Security, Auckland, July 7-12,* (pp. 295-306) New York: ACM. https://doi.org/10.1145/3321705.3329831 (Published)

ObliDC: An SGX-based oblivious distributed computing framework with formal proof, by WU, Pengfei; SHEN, Qingni; DENG, Robert H.; LIU, Ximeng; ZHANG, Yinghui; WU, Zhonghai. (2019.0). *AsiaCCS '19: Proceedings of the ACM Asia Conference on Information, Computer and Communications Security, Auckland, New Zealand, July 9-12,* (pp. 86-99) New York: ACM. https://doi.org/10.1145/3321705.3329822 (Published)

DroidEvolver: Self-evolving Android malware detection system, by XU, Ke; LI, Yingjiu; DENG, Robert H.; CHEN, Kai; XU, Jiayun. (2019.0). *Proceedings of the 4th IEEE European Symposium on Security and Privacy (EuroS&P 2019),* (pp. 47-62) Stockholm, Sweden: IEEE. (Published)

Understanding open ports in Android applications: Discovery, diagnosis, and security assessment, by WU, Daoyuan; GAO, Debin; CHANG, Rocky K. C.; HE, En; CHENG, Eric K. T.; DENG, Robert H.. (2019.0). *Network and Distributed System Security Symposium 26th NDSS 2019: February 24-27, San Diego, CA: Proceedings,* (pp. 1-14) Reston, VA: Internet Society. https://doi.org/10.14722/ndss.2019.23171 (Published)

Privacy-preserving remote user authentication with K-times untraceability, by TIAN, Yangguang; LI, Yingjiu; SENGUPTA, Binanda; DENG, Robert H.; CHING, Albert; LIU, Weiwei. (2018.0). *Information Security and Cryptology: 14th International Conference, Inscrypt 2018, Fuzhou, China, December 14-17: Proceedings,* (pp. 647-657) Cham: Springer. https://doi.org/10.1007/978-3-030-14234-6_36 (Published)

SybMatch: Sybil detection for privacy-preserving task matching in crowdsourcing, by SHU, Jiangang; LIU, Ximeng; YANG, Kan; ZHANG, Yinghui; JIA, Xiaohua; DENG, Robert H.. (2018.0). *2018 IEEE Global Communications Conference, GLOBECOM 2018, Abu Dhabi, United Arab Emirates, December 9-13: Proceedings,* (pp. 1-6) Piscataway, NJ: IEEE. https://doi.org/10.1109/GLOCOM.2018.8647346 (Published)

PriBioAuth: Privacy-preserving biometric-based remote user authentication, by TIAN, Yangguang; LI, Yingjiu; LIU, Ximeng; DENG, Robert H.; SENGUPTA, Binanda. (2018.0). *2018 IEEE Conference on*

*Dependable and Secure Computing DSC: Kaohsiung, Taiwan, December 10-13: Proceedings,* (pp. 112-132) Piscataway, NJ: IEEE. https://doi.org/10.1109/DESEC.2018.8625169 (Published)

Typing-Proof: Usable, secure and low-cost two-factor authentication based on keystroke timings, by LIU, Ximing; LI, Yingjiu; DENG, Robert H.. (2018.0). *ACSAC '18: Proceedings of the 34th Annual Computer Security Applications Conference, San Juan, Puerto Rico, December 3-7,* (pp. 53-65) New York: ACM. https://doi.org/10.1145/3274694.3274699 (Published)

PUSC: Privacy-preserving user-centric skyline computation over multiple encrypted domains, by LIU, Ximeng; CHOO, Kim-Kwang Raymond; DENG, Robert H.; YANG, Yang. (2018.0). *2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications / 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE): New York, August 1-3: Proceedings,* (pp. 958-963) Piscataway, NJ: IEEE. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00135 (Published)

DeepRefiner: Multi-layer Android malware detection system applying deep neural networks, by XU, Ke; LI, Yingjiu; DENG, Robert H.; CHEN, Kai. (2018.0). *3rd IEEE European Symposium on Security and Privacy Workshops EUROS&PW 2018: Proceedings: 24-26 April, London,* (pp. 473-487) Piscataway, NJ: IEEE. https://doi.org/10.1109/EuroSP.2018.00040 (Published)

SCLib: A practical and lightweight defense against component hijacking in Android applications, by WU, Daoyuan; CHENG, Yao; GAO, Debin; LI, Yingjiu; DENG, Robert H.. (2018.0). *CODASPY '18: Proceedings of 8th ACM Conference on Data and Application Security and Privacy, Tempe, AZ, March 19-21,* (pp. 299-306) New York: ACM. https://doi.org/10.1145/3176258.3176336 (Published)

VuRLE: Automatic vulnerability detection and repair by learning from examples, by MA, Siqi; THUNG, Ferdian; LO, David; SUN, Cong; DENG, Robert H.. (2017.0). *Computer security ESORICS 2017: 22nd European Symposium on Research in Computer Security, Oslo, Norway, September 11-15: Proceedings,* (pp. 229-246) Cham: Springer. https://doi.org/10.1007/978-3-319-66399-9_13 (Published)

Secure encrypted data deduplication with ownership proof and user revocation, by DING, Wenxiu; YAN, Zheng; DENG, Robert H.. (2017.0). *Algorithms and architectures for parallel processing: 17th International Conference ICA3PP 2017, Helsinki, Finland, August 21-23, Proceedings,* (pp. 297-312) Cham: Springer. https://doi.org/10.1007/978-3-319-65482-9_20 (Published)

Fair deposits against double-spending for Bitcoin transactions, by YU, Xingjie; THANG Shiwen M.; LI, Yingjiu; DENG, Robert H.. (2017.0). *2017 IEEE Conference on Dependable and Secure Computing: Taipei, Taiwan, August 7-10: Proceedings,* (pp. 44-51) Piscataway, NJ: IEEE. https://doi.org/10.1109/DESEC.2017.8073796 (Published)

Attribute-based encryption with expressive and authorized keyword search, by CUI, Hui; DENG, Robert H.; LIU, Joseph K.; LI, Yingjiu. (2017.0). *Information Security and Privacy: ACISP 2017: Auckland, New Zealand, July 3-5: Proceedings,* (pp. 106-126) Cham: Springer. https://doi.org/10.1007/978-3-319-60055-0_6 (Published)

What you see is not what you get: Leakage-resilient password entry schemes for smart glasses, by LI, Yan; CHENG, Yao; LI, Yingjiu; DENG, Robert H.. (2017.0). *ASIA CCS 2017: Proceedings of the ACM Asia Conference on Computer and Communications Security, April 2-6, Abu Dhabi, United Arab Emirates,* (pp. 327-333) New York: ACM. https://doi.org/10.1145/3052973.3053042 (Published)

Attribute-based secure messaging in the public cloud, by POH, Zhi Yuan; CUI, Hui; DENG, Robert H.; LI, Yingjiu. (2017.0). *A systems approach to cyber security: Proceedings of the 2nd Singapore Cyber-Security R&D Conference (SG-CRC 2017), February 21-22,* (pp. 86-96) Amsterdam: IOS Press. https://doi.org/10.3233/978-1-61499-744-3-86 (Published)

H-Binder: A hardened binder framework on Android systems, by SHEN, Dong; ZHANG, Zhangkai; DING, Xuhua; LI, Zhoujun; DENG, Robert H.. (2017.0). *Security and privacy in communication networks: 12th International Conference, SecureComm 2016, Guangzhou, China, October 10-12, Proceedings,* (pp. 24-43) Cham: Springer. https://doi.org/10.1007/978-3-319-59608-2_2 (Published)

An efficient and expressive ciphertext-policy attribute-based encryption scheme with partially hidden access structures, by CUI, Hui; DENG, Robert H.; WU, Guowei; LAI, Junzuo. (2016.0). *Provable security: 10th International Conference, ProvSec 2016, Nanjing, China, November 10-11, Proceedings,* (pp. 19-38) Cham: Springer. https://doi.org/10.1007/978-3-319-47422-9_2 (Published)

Attribute-based encryption with granular revocation, by CUI, Hui; DENG, Robert H.; DING, Xuhua; LI,

Yingjiu. (2016.0). *Security and Privacy in Communication Networks: 12th International Conference, SecureComm 2016, Guangzhou, China, October 10-12: Proceedings,* (pp. 165-181) Cham: Springer. https://doi.org/10.1007/978-3-319-59608-2_9 (Published)

Server-aided revocable attribute-based encryption, by CUI, Hui; DENG, Robert H.; LI, Yingjiu; QIN, Baodong. (2016.0). *Computer security ESORICS 2016: 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26-30: Proceedings,* (pp. 570-587) Cham: Springer. https://doi.org/10.1007/978-3-319-45741-3_29 (Published)

Generic anonymous identity-based broadcast encryption with chosen-ciphertext security, by HE, Kai; WENG, Jian; AU, Man Ho; MAO, Yijun; DENG, Robert H.. (2016.0). *Information Security and Privacy: 21st Australasian Conference, ACISP 2016, Melbourne, July 4-6, 2016, Proceedings,* (pp. 207-222) Cham: Springer. https://doi.org/10.1007/978-3-319-40367-0_13 (Published)

A feasible no-root approach on Android, by CHENG, Yao; LI, Yingjiu; DENG, Robert H.. (2016.0). *Information Security and Privacy: Proceedings of the 21st Australasian Conference on Information Security and Privacy (ACISP): Melbourne, Australia, July 4-6,* (pp. 481-489) Cham: Springer. https://doi.org/10.1007/978-3-319-40367-0_32 (Published)

Anonymous identity-based broadcast encryption with chosen-ciphertext security, by HE, Kai; WENG, Jian; LIU, Jia-Nan; LIU, Joseph K.; LIU, Wei; DENG, Robert H.. (2016.0). *ASIA CCS'16: Proceedings of the 11th ACM Asia Conference on Computer and Communications Security: Xi'an, China, May 30-June 3,* (pp. 247-255) New York: ACM. https://doi.org/10.1145/2897845.2897879 (Published)

CDRep: Automatic repair of cryptographic-misuses in Android applications, by MA, Siqi; LO, David; LI, Teng; DENG, Robert H.. (2016.0). *ASIA CCS '16: Proceedings of the 11th ACM Asia Conference on Computer and Communications Security: May 30 - June 3, Xi'an, China,* (pp. 711-722) New York: ACM. https://doi.org/10.1145/2897845.2897896 (Published)

Efficient verifiable computation of linear and quadratic functions over encrypted data, by TRAN, Ngoc Hieu; PANG, Hwee Hwa; DENG, Robert H.. (2016.0). *Asia CCS '16: Proceedings of the 11th ACM Asia Conference on Computer and Communications Security, Xi'an, China, May 30 - June 3,* (pp. 605-616) New York: ACM. https://doi.org/10.1145/2897845.2897892 (Published)

CCA-secure keyed-fully homomorphic encryption, by LAI, Junzuo; DENG, Robert H.; MA, Changshe; SAKURAI, Kouichi; WENG, Jian. (2016.0). *Proceedings of the 19th International Conference on the Theory and Practice of Public-Key Cryptography (PKC 2016):,* (pp. 70-98) Taiwan: Springer. http://doi.org/10.1007/978-3-662-49384-7_4 (Published)

Privacy-preserving and verifiable data aggregation, by TRAN, Ngoc Hieu; DENG, Robert H.; PANG, Hwee Hwa. (2016.0). *Proceedings of the Singapore Cyber-Security Conference (SG-CRC) 2016: Singapore, January 14-15,* (pp. 115-122) Amsterdam: IOS Press. https://doi.org/10.3233/978-1-61499-617-0-115 (Published)

Electronic contract signing without using trusted third party, by WAN, Zhiguo; DENG, Robert H.; LEE, David. (2015.0). *Network and System Security: 9th International Conference, NSS 2015, New York, November 3-5, Proceedings,* (pp. 386-394) Cham: Springer. https://doi.org/10.1007/978-3-319-25645-0_27 (Published)

Seeing your face is not enough: An inertial sensor-based liveness detection for face authentication, by LI, Yan; LI, Yingjiu; YAN, Qiang; KONG, Hancong; DENG, Robert H.. (2015.0). *CCS 15: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, October 12-16,* (pp. 1558-1569) New York: ACM. https://doi.org/10.1145/2810103.2813612 (Published)

On security of content-based video stream authentication, by LO, Swee-Won; WEI, Zhou; DENG, Robert H.; DING, Xuhua. (2015.0). *Computer Security – ESORICS 2015: 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, Proceedings,* (pp. 366-383) Cham: Springer. http://dx.doi.org/10.1007/978-3-319-24174-6_19 (Published)

Server-aided revocable identity-based encryption, by QIN, Baodong; DENG, Robert H.; LI, Yingjiu; LIU, Shengli. (2015.0). *Computer Security – ESORICS 2015: 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I,* (pp. 286-304) Vienna, Austria: Springer. https://doi.org/10.1007/978-3-319-24174-6_15 (Published)

Active Semi-supervised Approach for Checking App Behavior against its Description, by MA, Siqi; WANG, Shaowei; LO, David; DENG, Robert H.; SUN, Cong. (2015.0). *2015 IEEE 39th Annual Computers Software*

*and Applications Conference (COMPSAC): 1-5 July 2015, Taichung, Taiwan: Proceedings,* (pp. 179-184) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/COMPSAC.2015.93 (Published)

CICC: A Fine-grained, Semantic-aware, and Transparent Approach to Preventing Permission Leaks for Android Permission Managers, by WANG, Daibin; YAO, Haixia; LI, Yingjiu; JIN, Hai; ZOU, Deqing; DENG, Robert H.. (2015.0). *WiSec '15: Proceedings of the 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks, June 22-26, 2015, New York,* (pp. 1-6) New York: ACM. http://dx.doi.org/10.1145/2766498.2766518 (Published)

Continuous non-malleable key derivation and its application to related-key security, by QIN, Baodong; LIU, Shenli; YUEN, Tsz Hon; DENG, Robert H.; CHEN, Kefei. (2015.0). *Public-Key Cryptography - PKC 2015: 18th IACR International Conference on Practice and Theory in Public-Key Cryptography, Gaithersburg, MD, USA, March 30 - April 1, 2015, Proceedings,* (pp. 557-578) Cham: Springer. https://doi.org/10.1007/978-3-662-46447-2_25 (Published)

Efficient Virtualization-based Application Protection against Untrusted Operating System, by CHENG, Yueqiang; DING, Xuhua; DENG, Robert H.. (2015.0). *AsiaCCS'15: Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security: April 14-17, 2015, Singapore,* (pp. 345-356) New York: ACM. http://dx.doi.org/10.1145/2714576.2714618 (Published)

Multidimensional context awareness in mobile devices, by WEI, Zhou; DENG, Robert H.; SHEN, Jialie; ZHU, Jixiang; OUYANG, Kun; WU, Yongdong. (2015.0). *MultiMedia Modeling: 21st International Conference, MMM 2015, Sydney, NSW, Australia, January 5-7: Proceedings,* (pp. 38-49) Cham: Springer. https://doi.org/10.1007/978-3-319-14442-9_4 (Published)

Android or iOS for better privacy protection?, by HAN, Jin; YAN, Qiang; GAO, Debin; ZHOU, Jianying; DENG, Robert H.. (2014.0). *International Conference on Secure Knowledge Management in Big-data Era SKM 2014, Dubai, UAE, 8-9 December,* Dubai, UAE: BITS Pilani. (Published)

Detecting camouflaged applications on mobile application markets, by SU, Mon Kywe; LI, Yingjiu; DENG, Robert H.; Hong, Jason. (2014.0). *Information Security and Cryptology ICISC 2014: 17th International Conference, Seoul, South Korea, December 3-5, Revised Selected Papers,* (pp. 241-254) Cham: Springer. https://doi.org/10.1007/978-3-319-15943-0_15 (Published)

Verifiable computation on outsourced encrypted data, by LAI, Junzuo; DENG, Robert H.; PANG, Hwee Hwa; WENG, Jian. (2014.0). *Computer Security - ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11: Proceedings, Part I,* (pp. 273-291) Cham: Springer. https://doi.org/10.1007/978-3-319-11203-9_16 (Published)

Authorized keyword search on encrypted data, by SHI, Jie; LAI, Junzuo; LI, Yingjiu; DENG, H. Robert; WENG, Jian. (2014.0). *Computer Security - ESORICS 2014: 19th European Symposium on Research in Computer Security, Wroclaw, Poland, September 7-11: Proceedings, Part I,* (pp. 419-435) Cham: Springer. https://doi.org/10.1007/978-3-319-11203-9_24 (Published)

Understanding OSN-based Facial Disclosure against Face Authentication Systems, by LI, Yan; XU, Ke; YAN, Qiang; LI, Yingjiu; DENG, Robert H.. (2014.0). *ASIA CCS '14: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, June 4-6, 2014, Kyoto,* (pp. 413-424) New York: ACM. http://dx.doi.org/10.1145/2590296.2590315 (Published)

Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption, by LAI, Junzuo; DENG, H. Robert; LI, Yingjiu; WENG, Jian. (2014.0). *ASIA CCS'14: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security: Kyoto, Japan, June 4-6,* (pp. 239-248) New York: ACM. https://doi.org/10.1145/2590296.2590334 (Published)

Identity-based encryption secure against selective opening chosen-ciphertext attack, by LAI, Junzuo; DENG, Robert H.; LIU, Shengli; WENG, Jian; ZHAO, Yunlei. (2014.0). *Advances in Cryptology EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, Proceedings,* (pp. 77-92) Heidelberg: Springer. https://doi.org/10.1007/978-3-642-55220-5_5 (Published)

ROPecker: A generic and practical approach for defending against ROP attack, by CHENG, Yueqiang; ZHOU, Zongwei; MIAO, Yu; DING, Xuhua; DENG, Robert H.. (2014.0). *NDSS Symposium 2014: Proceedings of the 21st Network and Distributed System Security Symposium, San Diego, February 23-26,* (pp. 1-14) Reston, VA: Internet Society. https://doi.org/10.14722/ndss.2014.23156 (Published)

Adaptable ciphertext-policy attribute-based encryption, by LAI, Junzuo; DENG, Robert H.; YANG, Yanjiang;

Weng, Jian. (2013.0). *Pairing-Based Cryptography - Pairing 2013: 6th International Conference, Beijing, China, November 22-24: Revised Selected Papers,* (pp. 199-214) Berlin: Springer. https://doi.org/10.1007/978-3-319-04873-4_12 (Published)

Technique for authenticating H.264/SVC streams in surveillance applications, by ZHUO, Wei; DENG, Robert H.; SHEN, Jialie; WU, Yongdong; DING, Xuhua; LO, Swee Won. (2013.0). *Electronic Proceedings of the 2013 IEEE International Conference on Multimedia and Expo Workshops (ICMEW 2013): 15-19 July, 2013, San Jose, California,* (pp. 1-14) Los Alamitos, CA: IEEE Computer Society. http://doi.ieeecomputersociety.org/10.1109/ICMEW.2013.6618259 (Published)

Launching generic attacks on iOS with approved third-party applications, by HAN, Jin; SU, Mon Kywe; YAN, Qiang; BAO, Feng; DENG, Robert H.; GAO, Debin; LI, Yingjiu; ZHOU, Jianying. (2013.0). *Applied Cryptography and Network Security: 11th International Conference, ACNS 2013, Banff, AB, Canada, June 25-28: Proceedings,* (pp. 272-289) Berlin: Springer. https://doi.org/10.1007/978-3-642-38980-1_17 (Published)

Privacy leakage analysis in online social networks, by LI, YAN; LI, Yingjiu; YAN, Qiang; DENG, Robert H.. (2015.0). *Proceedings of NSS: Network and System Security: NSS 2013, Madrid, Spain, June 3-4: Proceedings,* (pp. 671-677) Berlin: Springer. https://doi.org/10.1007/978-3-642-38631-2_55 (Published)

Anonymous authentication of visitors for mobile crowd sensing at amusement parks, by KONIDALA, Divyan; DENG, Robert H.; LI, Yingjiu; LAU, Hoong Chuin; FIENBERG, Stephen. (2013.0). *Information Security Practice and Experience: 9th International Conference, ISPEC 2013, Lanzhou, China, May 12-14: Proceedings,* (pp. 174-188) Cham: Springer. https://doi.org/10.1007/978-3-642-38033-4_13 (Published)

Designing leakage-resilient password entry on touchscreen mobile devices, by YAN, Qiang; Han, JIN; LI, Yingjiu; ZHOU, Jianying; DENG, Robert H.. (2013.0). *ASIA CCS '13: Proceedings of the 8th ACM SIGSAC symposium on Information, Computer and Communications Security: May 8-10, Hangzhou, China,* (pp. 37-48) New York: ACM. https://doi.org/10.1145/2484313.2484318 (Published)

Expressive search on encrypted data, by LAI, Junzuo; ZHOU, Xuhua; DENG, Robert H.; LI, Yingjiu; CHEN, Kefei. (2013.0). *ASIA CCS '13: Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security: May 8-10, Hangzhou, China,* (pp. 243-252) New York: ACM. https://doi.org/10.1145/2484313.2484345 (Published)

Accountable authority identity-based encryption with public traceability, by LAI, Junzuo; DENG, Robert H.; ZHAO, Yunlei; WENG, Jian. (2013.0). *Topics in Cryptology - CT-RSA 2013: The Cryptographers' Track at the RSA Conference, San Francisco,CA, February 25-March 1: Proceedings,* (pp. 324-342) Cham: Springer. https://doi.org/10.1007/978-3-642-36095-4_21 (Published)

Comparing Mobile Privacy Protection through Cross-Platform Applications, by HAN, Jin; YAN, QIANG; GAO, Debin; ZHOU, Jianying; DENG, Robert H.. (2013.0). *Proceedings of NDSS 2013: Network and Distributed System Security Symposium, 24-27 February, San Diego,* Reston, VA: Internet Society. http://www.internetsociety.org/doc/comparing-mobile-privacy-protection-through-cross-platform-applications (Published)

An improved authentication scheme for H.264/SVC and its performance evaluation over non-stationary wireless mobile networks, by ZHAO, Yifan; LO, Swee-Won; DENG, Robert H.; DING, Xuhua. (2012.0). *Network and System Security: 6th International Conference, NSS 2012, Wuyishan, Fujian, China, November 21-23, Proceedings,* (pp. 192-206) Cham: Springer. https://doi.org/10.1007/978-3-642-34601-9_15 (Published)

Design and Implementation of a Secure Prototype for EPCglobal Network Services, by SHI, Jie; LI, Yingjiu; DENG, Robert H.; CHIEW, Kevin. (2012.0). *Radio Frequency Identification System Security: RFIDsec'12 Asia Workshop Proceedings: Taipei, Taiwan, November 8-9, 2012,* (pp. 45-56) Amsterdam: IOS Press. http://dx.doi.org/10.3233/978-1-61499-143-4-45 (Published)

No tradeoff between confidentiality and performance: An analysis on H.264/SVC partial encryption, by WEI, Zhuo; DING, Xuhua; DENG, Robert H.; WU, Yongdong. (2012.0). *Communications and multimedia security: 13th IFIP TC 6/TC 11 International Conference, CMS 2012, Canterbury, September 3-5: Proceedings,* (pp. 72-86) Cham: Springer. https://doi.org/10.1007/978-3-642-32805-3_6 (Published)

A Pollution Attack to Public-key Watermarking Schemes, by WU, Yongdong; DENG, Robert H.. (2012.0). *IEEE International Conference on Multimedia and Expo (ICME) 2012: 9-13 July 2012, Melbourne, Australia: Proceedings,* (pp. 230-235) Los Alamitos, CA: IEEE Computer Society. http://doi.ieeecomputersociety.org/10.1109/ICME.2012.73 (Published)

A new framework for privacy of RFID path authentication, by CAI, Shaoying; DENG, Robert H.; LI, Yingjiu; ZHAO, Yunlei. (2012.0). *Applied Cryptography and Network Security: 10th International Conference, ACNS 2012, Singapore, June 26-29: Proceedings,* (pp. 473-488) Berlin: Springer. https://doi.org/10.1007/978-3-642-31284-7_28 (Published)

Expressive CP-ABE with partially hidden access structures, by LAI, Junzuo; DENG, Robert H.; LI, Yingjiu. (2012.0). *AsiaCCS 2012: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, May 2-4, Seoul, Korea,* (pp. 18-19) New York: ACM. http://dx.doi.org/10.1145/2414456.2414465 (Published)

A secure and efficient discovery service system in EPCglobal network, by SHI, Jie; SIM, Darren; LI, Yingjiu; DENG, Robert H.. (2012.0). *CODASPY '12: Proceedings of the 2nd ACM Conference on Data and Application Security and Privacy, February 7-9, 2012, San Antonio, TX,* (pp. 267-274) New York: ACM. http://dx.doi.org/10.1145/2133601.2133634 (Published)

On limitations of designing usable leakage-resilient password systems: Attacks, principles and usability, by YAN, Qiang; Han, JIN; LI, Yingjiu; DENG, Robert H.. (2012.0). *Proceedings of the 19th Annual Network & Distributed System Security Symposium, San Diego, CA, 2012 February 5-8,* (pp. 1-16) Reston, VA: Internet Society. (Presented)

Applying time-bound hierarchical key assignment in wireless sensor networks, by ZHU, Wentao; DENG, Robert H.; ZHOU, Jianying; BAO, Feng. (2011.0). *Information and Communications Security: 13th International Conference, ICICS 2011, Beijing, China, November 23-26: Proceedings,* (pp. 306-318) Berlin: Springer. https://doi.org/10.1007/978-3-642-25243-3_25 (Published)

Zero-error watermarking on JPEG images by shuffling Huffman tree nodes, by WU, Yongdong; DENG, Robert H.. (2011.0). *2011 IEEE Visual Communications and Image Processing VCIP: November 6-9, 2011: Tainan City, Taiwan: Proceedings,* (pp. 1-4) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/VCIP.2011.6115939 (Published)

General construction of chameleon all-but-one trapdoor functions, by LIU, Shengli; LAI, Junzuo; DENG, Robert H.. (2011.0). *Provable Security: 5th International Conference, ProvSec 2011, Xi'an, China, October 16-18: Proceedings,* (pp. 257-265) Heidelberg: Springer. https://doi.org/10.1007/978-3-642-24316-5_18 (Published)

DriverGuard: A fine-grained protection on I/O flow, by CHENG, Yueqiang; DING, Xuhua; DENG, Robert H.. (2011.0). *Computer Security – ESORICS 2011: 16th European Symposium on Research in Computer Security, Leuven, Belgium, September 12-14,* (pp. 227-244) Berlin: Springer. https://doi.org/10.1007/978-3-642-23822-2_13 (Published)

On detection of erratic arguments, by HAN, Jin; YAN, Qiang; DENG, Robert H.; GAO, Debin. (2011.0). *Security and Privacy in Communication Networks: 7th International ICST Conference, SecureComm 2011, London, UK, September 7-9, Revised Selected Papers,* (pp. 172-189) Heidelberg: Springer. https://doi.org/10.1007/978-3-642-31909-9_10 (Published)

Hierarchical identity-based chameleon hash and its applications, by BAO, Feng; DENG, Robert H.; DING, Xuhua; LAI, Junzuo; ZHAO, Yunlei. (2011.0). *Applied Cryptography and Network Security: 9th International Conference, ACNS 2011, Nerja, Spain, June 7-10: Proceedings,* (pp. 201-219) Berlin: Springer. https://doi.org/10.1007/978-3-642-21554-4_12 (Published)

Fully secure cipertext-policy hiding CP-ABE, by LAI, Junzuo; DENG, Robert H.; LI, Yingjiu. (2011.0). *Information Security Practice and Experience: 7th International Conference, ISPEC 2011, Guangzhou, China, May 30 - June 1: Proceedings,* (pp. 24-39) Heidelberg: Springer. https://doi.org/10.1007/978-3-642-21031-0_3 (Published)

RFID mutual authentication protocols with universally composable security, by SU, Chunhua; LI, Yingjiu; DENG, Robert H.. (2011.0). *Proceedings of Workshop on Radio Frequency Identification System Security, Peking Univ, Wuxi, China, 2011 April 6-8,* (pp. 35-49) Peking Univ, Wuxi, China: https://doi.org/10.3233/978-1-60750-722-2-35 (Published)

Secure mobile subscription of sensor-encrypted data, by CHU, Cheng-Kang; ZHU, Wen-Tao; CHOW, Sherman S. M.; ZHOU, Jianying; DENG, Robert H.. (2011.0). *ASIACCS '11: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security: Hong Kong, March 22-24,* (pp. 228-237) New York: ACM. https://doi.org/10.1145/1966913.1966943 (Published)

Chameleon all-but-one TDFs and their application to chosen-ciphertext security, by LAI, Junzuo; DENG, Robert H.; LIU, Shengli. (2011.0). *Public Key Cryptography - PKC 2011: 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, March 6-9, 2011: Proceedings,* (pp. 228-245) Heidelberg: Springer. https://doi.org/10.1007/978-3-642-19379-8_14 (Published)

Protecting and restraining the third party in RFID-enabled 3PL supply chains, by CAI, Shaoying; SU, Chunhua; LI, Yingjiu; DENG, Robert H.. (2010.0). *Information Systems Security: 6th International Conference, ICISS 2010, Gandhinagar, India, December 17-19: Proceedings,* (pp. 246-260) Berlin: Springer. https://doi.org/10.1007/978-3-642-17714-9_18 (Published)

Time cost evaluation for executing RFID authentication protocols, by CHIEW, Kevin; LI, Yingjiu; LI, Tieyan; DENG, Robert H.; AIGNER, Manfred. (2010.0). *2010 Internet of Things: IOT, Tokyo, Japan, November 29 - December 1: Proceedings,* (pp. 1-8) Piscataway, NJ: IEEE. https://doi.org/10.1109/IOT.2010.5678437 (Published)

A new framework for RFID privacy, by DENG, Robert H.; LI, Yingjiu; YUNG, Moti; ZHAO, Yunlei. (2010.0). *Computer Security: ESORICS 2010: 15th European Symposium on Research in Computer Security, Athens, Greece, September 20-22: Proceedings,* (pp. 1-18) Berlin: Springer. https://doi.org/10.1007/978-3-642-15497-3_1 (Published)

Pseudonym-based RFID Discovery Service to mitigate unauthorized tracking in supply chain management, by YAN, Qiang; DENG, Robert H.; YAN, Zheng; LI, Yingjiu; LI, Tieyan. (2010.0). *ISDPE '10: Proceedings of the 2010 Second International Symposium on Data, Privacy, and E-Commerce, Buffalo, New York, 13-14 September 2010,* (pp. 21-26) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/ISDPE.2010.9 (Published)

Revisiting unpredictability-based RFID privacy models, by LAI, Junzuo; DENG, Robert H.; LI, Yingjiu. (2010.0). *Applied Cryptography and Network Security: 8th International Conference, ACNS 2010, Beijing, China, June 22-25: Proceedings,* (pp. 475-492) Berlin: Springer. https://doi.org/10.1007/978-3-642-13708-2_28 (Published)

Efficient unidirectional proxy re-encryption, by CHOW, Sherman S. M.; JIAN, Weng; YANG, Yanjiang; DENG, Robert H.. (2010.0). *Progress in Cryptology - AFRICACRYPT 2010: Third International Conference on Cryptology in Africa, Stellenbosch, South Africa, May 3-6: Proceedings,* (pp. 316-332) Berlin: Springer. https://doi.org/10.1007/978-3-642-12678-9_19 (Published)

Practical ID-based encryption for wireless sensor network, by CHU, Cheng-Kang; LIU, Joseph K.; ZHOU, Jianying; BAO, Feng; DENG, Robert H.. (2010.0). *ASIACCS '10: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, April 13-16, Beijing,* (pp. 337-340) New York: ACM. https://doi.org/10.1145/1755688.1755734 (Published)

Efficient CCA-secure PKE from identity-based techniques, by LAI, Junzuo; DENG, Robert H.; LIU, Shengli; KOU, Weidong. (2010.0). *Topics in Cryptology - CT-RSA 2010: The Cryptographers' Track at the RSA Conference 2010, San Francisco, CA, March 1-5: Proceedings,* (pp. 132-147) Berlin: Springer. https://doi.org/10.1007/978-3-642-11925-5_10 (Published)

Remote attestation on function execution, by GU, Liang; CHENG, Yueqiang; DING, Xuhua; DENG, Robert H.; GUO; Yao; SHAO, Weizhong. (2010.0). *Trusted Systems: First International Conference, INTRUST 2009, Beijing, China, December 17-19: Revised Selected Papers,* (pp. 60-72) Berlin: Springer. https://doi.org/10.1007/978-3-642-14597-1_4 (Published)

On the untraceability of anonymous RFID authentication protocol with constant key-lookup, by LIANG, Bing; LI, Yingjiu; LI, Tieyan; DENG, Robert H.. (2009.0). *Information Systems Security: 5th International Conference, ICISS 2009 Kolkata, India, December 14-18: Proceedings,* (pp. 71-85) Berlin: Springer. https://doi.org/10.1007/978-3-642-10772-6_7 (Published)

Computationally secure hierarchical self-healing key distribution for heterogeneous wireless sensor networks, by YANG, Yanjiang; ZHOU, Jianying; DENG, Robert H.; BAO, Feng. (2009.0). *Information and Communications Security: 11th International Conference, ICICS 2009, Beijing, China, December 14-17: Proceedings,* (pp. 135-149) Berlin: Springer. https://doi.org/10.1007/978-3-642-11145-7_12 (Published)

Enabling secure secret updating for unidirectional key distribution in RFID-enabled supply chains, by CAI, Shaoying; LI, Tieyan; MA, Changshe; LI, Yingjiu; DENG, Robert H.. (2009.0). *Information and Communications Security: 11th International Conference, ICICS 2009, Beijing, China, December 14-17: Proceedings,* (pp. 150-164) Berlin: Springer. https://doi.org/10.1007/978-3-642-11145-7_13 (Published)

Insights into malware detection and prevention on mobile phones, by YAN, Qiang; LI, Yingjiu; LI, Tieyan; DENG, Robert H.. (2009.0). *Security Technology: International Conference, SecTech 2009, Jeju Island, Korea, December 10-12: Proceedings,* (pp. 242-249) Berlin: Springer. https://doi.org/10.1007/978-3-642-10847-1_30 (Published)

Fooling Public-Key Watermarking Detectors with Optimal Color Noise, by WU, Yongdong; DENG, Robert H.. (2009.0). *MINES '09: International Conference on Multimedia Information Networking and Security: 18-20 November 2009, Hubei, China: Proceedings,* (pp. 5-9) Los Alamitos, CA: IEEE Computer Society. http://doi.ieeecomputersociety.org/10.1109/MINES.2009.129 (Published)

On Group Key Management for Secure Multicast Employing the Inverse Element, by ZHU, Wen Tao; DENG, Robert H.. (2009.0). *MINES '09: International Conference on Multimedia Information Networking and Security, 18-20 November 2009, Hubei, China: Proceedings,* (pp. 337-341) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/MINES.2009.56 (Published)

Secure mobile agents with designated hosts, by ZHANG, Qi; MU, Yi; ZHANG, Minji; DENG, Robert H.. (2009.0). *NSS '09: Third International Conference on Network and System Security: Gold Coast, Queensland, Australia, 19-21 October 2009,* (pp. 286-293) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/NSS.2009.59 (Published)

Hierarchical self-healing key distribution for heterogeneous wireless sensor networks, by YANG, Yanjiang; ZHOU, Jianying; DENG, Robert H.; BAO, Feng. (2009.0). *Security and Privacy in Communication Networks: 5th International ICST Conference, SecureComm 2009, Athens, Greece, September 14-18: Revised Selected Papers,* (pp. 285-295) Berlin: Springer. https://doi.org/10.1007/978-3-642-05284-2_16 (Published)

RFID privacy: Relation between two notions, minimal condition, and efficient construction, by MA, Changshe; LI, Yingjiu; DENG, Robert H.; LI, Tieyan. (2009.0). *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS 2009), September 9-13, Chicago, Illinois,* (pp. 54-65) New York: ACM. http://dx.doi.org/10.1145/1653662.1653670 (Published)

Efficient conditional proxy re-encryption with chosen-ciphertext security, by WENG, Jian; YANG, Yanjiang; TANG, Qiang; DENG, Robert H.. (2009.0). *Information Security: 12th International Conference, ISC 2009, Pisa, Italy, September 7-9: Proceedings,* (pp. 151-166) Berlin: Springer. https://doi.org/10.1007/978-3-642-04474-8_13 (Published)

On the effectiveness of software diversity: A systematic study on real-world vulnerabilities, by HAN, Jin; GAO, Debin; DENG, Robert H.. (2009.0). *Detection of Intrusions and Malware, and Vulnerability Assessment: 6th International Conference, DIMVA 2009, Como, Italy, July 9-10: Proceedings,* (pp. 127-146) Berlin: Springer. https://doi.org/10.1007/978-3-642-02918-9_8 (Published)

Conditional proxy broadcast re-encryption, by CHU, Cheng-Kang; WENG, Jian; CHOW, Sherman S. M.; ZHOU, Jianying; DENG, Robert H.. (2009.0). *Information Security and Privacy: 14th Australasian Conference, ACISP 2009 Brisbane, Australia, July 1-3: Proceedings,* (pp. 327-242) Berlin: Springer. https://doi.org/10.1007/978-3-642-02620-1_23 (Published)

Applying sanitizable signature to web-service-enabled business processes: Going beyond integrity protection, by TAN, Kar Way; DENG, Robert H.. (2009.0). *ICWS 2009: IEEE 7th International Conference on Web Services, Los Angeles, CA, 6-10 July: Proceedings,* (pp. 67-74) Los Alamitos, CA: IEEE Computer Society. https://doi.ieeecomputersociety.org/10.1109/ICWS.2009.34 (Published)

Ensuring dual security modes in RFID-enabled supply chain systems, by CAI, Shaoying; LI, Tieyan; LI, Yingjiu; DENG, Robert H.. (2009.0). *Information Security and Trust: 5th International Conference, ISPEC 2009 Xi’ an, China, April 13-15: Proceedings,* (pp. 372-383) Berlin: Springer. https://doi.org/10.1007/978-3-642-00843-6_32 (Published)

Achieving better privacy protection in wireless sensor networks using trusted computing, by YANG, Yanjiang; DENG, Robert H.; Zhou, Jianying; QIU, Ying. (2009.0). *Information Security Practice and Experience: 5th International Conference, ISPEC 2009 Xi’ an, China, April 13-15: Proceedings,* (pp. 384-395) Berlin: Springer. https://doi.org/10.1007/978-3-642-00843-6_33 (Published)

RSA-based certificateless public key encryption, by LAI, Junzuo; DENG, Robert H.; LIU, Shengli; KOU, Weidong. (2009.0). *Information Security Practice and Experience: 5th International Conference ISPEC 2009, Xi'an, China, April 13-15: Proceedings,* (pp. 24-34) Berline: Springer. https://doi.org/10.1007/978-3-642-00843-6_3 (Published)

Conditional proxy re-encryption secure against chosen-ciphertext attacks, by WENG, Jian; DENG, Robert

H.; DING, Xuhua; CHU, Cheng-Kang; LAI, Junzuo. (2009.0). *ASIACCS '09: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, Sydney, Australia, March 10-12,* (pp. 322-332) New York: ACM. https://doi.org/10.1145/1533057.1533100 (Published)

Attacks and Improvements to an RFID Mutual Authentication Protocol, by CAI, Shaoying; LI, Yingjiu; LI, Tieyan; DENG, Robert H.. (2009.0). *Proceedings of the Second ACM Conference on Wireless Network Security WiSec '09: Zurich, Switzerland, March 16-18, 2009,* (pp. 51-58) ACM. http://dx.doi.org/10.1145/1514274.1514282 (Published)

Chosen-ciphertext secure proxy re-encryption without pairing, by DENG, Robert H.; WENG, Jian; LIU, Shengli; CHEN, Kefei. (2008.0). *Cryptology and Network Security: 7th International Conference, CANS 2008, Hong-Kong, December 2-4: Proceedings,* (pp. 1-17) Berlin: Springer. https://doi.org/10.1007/978-3-540-89641-8_1 (Published)

Efficient client-to-client password authenticated key exchange, by YANG, Yanjiang; BAO, Feng; DENG, Robert H.. (2008.0). *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, EUC 2008: 17-20 December, Shanghai, China: Proceedings,* (pp. 202-207) Piscataway, NJ: IEEE. https://doi.org/10.1109/EUC.2008.32 (Published)

Model-driven remote attestation: Attesting remote system from behavioral aspect, by GU, Liang; DING, Xuhua; DENG, Robert H.; ZOU Yanzhen; XIE, Bing; SHAO, Weizhong; MEI, Hong. (2008.0). *2008 ICYCS 9th International Conference for Young Computer Scientists: November 18-21, Zhang Jia Jie, Hunan, China: Proceedings,* (pp. 2347-2353) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/ICYCS.2008.349 (Published)

Remote attestation on program execution, by GU, Liang; DING, Xuhua; DENG, Robert H.; XIE, Bing; MEI, Hong. (2008.0). *Proceedings of the 3rd ACM Workshop on Scalable Trusted Computing, Alexandria, Virginia, October 31,* (pp. 11-20) New York: ACM. https://doi.org/10.1145/1456455.1456458 (Published)

Using trusted computing technology to facilitate security enforcement in wireless sensor networks, by YANG, Yanjiang; DENG, Robert H.; BAO, Feng; ZHOU, Jianying. (2008.0). *APTC 2008: Proceedings of the 3rd Asia-Pacific Trusted Infrastructure Technologies Conference: 14-17 October, Wuhan,* (pp. 43-52) Piscataway, NJ: IEEE. https://doi.org/10.1109/APTC.2008.13 (Published)

An efficient PIR construction using trusted hardware, by YANG, Yanjiang; DING, Xuhua; DENG, Robert H.; BAO, Feng. (2008.0). *Information Security: 11th International Conference, ISC 2008, Taipei, Taiwan, September 15-18: Proceedings,* (pp. 64-79) Berlin: Springer. https://doi.org/10.1007/978-3-540-85886-7_5 (Published)

Distinguishing between FE and DDoS using randomness check, by PARK, Hyundo; LI, Peng; GAO, Debin; LEE, Heejo; DENG, Robert H.. (2008.0). *Information security: 11th International Conference, ISC 2008, Taipei, Taiwan, September 15-18, Proceedings,* (pp. 131-145) Berlin: Springer. https://doi.org/10.1007/978-3-540-85886-7_9 (Published)

Scalable RFID Authentication and Discovery in EPCglobal Network, by LI, Tieyan; DENG, Robert H.. (2008.0). *ChinaCom 2008: Third International Conference on Communications and Networking in China: August 25-27, Hangzhou, China: Proceedings,* (pp. 1138-1142) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/CHINACOM.2008.4685227 (Published)

A real-time tele-ophalmology system based on secure video-conferencing and white-board, by YU, Shengsheng; WEI, Zhuo; DENG, Robert H.; YAO, Haixia; ZHAO, Zhigang; NGOH, Lek Heng; WU, Yongdong. (2008.0). *2008 10th IEEE International Conference on e-Health Networking, Applications and Services HealthCom: Singapore, 7-9 July,* (pp. 51-52) Piscataway, NJ: IEEE. https://doi.org/10.1109/HEALTH.2008.4600109 (Published)

Robust and reliable broadcast protocols in the stand-alone and simulation-based frameworks, by ZHU, Huafei; BAO, Feng; DENG, Robert H.. (2008.0). *Proceedings of the 2008 IEEE International Conference on Communications, 19-23 May, Beijing,* (pp. 1635-1641) Piscataway, NJ: IEEE. https://doi.org/10.1109/ICC.2008.316 (Published)

Private query on encrypted data in multi-user setting, by BAO, Feng; DENG, Robert H.; DING, Xuhua; YANG, Yanjiang. (2008.0). *Information Security Practice and Experience: 4th International Conference, ISPEC 2008, Sydney, Australia, April 21-23: Proceedings,* (pp. 71-85) Berlin: Springer. https://doi.org/10.1007/978-3-540-79104-1_6 (Published)

nPAKE+: A hierarchical group password-authenticated key exchange protocol using different passwords,

by WAN, Zhiguo; DENG, Robert H.; BAO, Feng; PRENEEL, Bart. (2007.0). *Information and Communications Security: 9th International Conference, ICICS 2007, Zhengzhou, China, December 12-15: Proceedings,* (pp. 31-43) Berlin: Springer. https://doi.org/10.1007/978-3-540-77048-0_3 (Published)

Light-weight encryption schemes for multimedia data, by BAO, Feng; DENG, Robert H.. (2007.0). *GLOBECOM '07: IEEE Global Telecommunications Conference, 2007: Proceedings: Washington, DC, 26-30 November,* (pp. 188-192) Piscataway, NJ: IEEE. https://doi.org/10.1109/GLOCOM.2007.43 (Published)

An information-sharing based anti-phishing system, by CHENG, Yueqing; YUAN, Zhen; MA, lei; DENG, Robert H.. (2007.0). *Proceedings of the 1st International Symposium on Data, Privacy and E-Commerce, Chengdu, China, 2007 November 1-3,* (pp. 265-270) Chengdu, China: https://doi.org/10.1109/ISDPE.2007.65 (Published)

Enhanced security by OS-oriented encapsulation in TMP-enabled DRM, by WU, Yongdong; BAO, Feng; DENG, Robert H.; MOUFFRON, Marc; ROUSSEAU, Frederic. (2007.0). *Information Security and Cryptology: Third SKLOIS Conference, Inscrypt 2007, Xining, China, August 31 - September 5,* (pp. 472-481) Berlin: Springer. https://doi.org/10.1007/978-3-540-79499-8_37 (Published)

New paradigm of inference control with trusted computing, by YANG, Yanjiang; LI, Yingjiu; DENG, Robert H.. (2007.0). *Data and Applications Security XXI: 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security, Redondo Beach, CA, July 8-11, 2007: Proceedings,* (pp. 243-258) Berlin: Springer. https://doi.org/10.1007/978-3-540-73538-0_18 (Published)

Forgery attack to an asymptotically optimal traitor tracing scheme, by WU, Yongdong; BAO, Feng; DENG, Robert H.. (2007.0). *Information Security and Privacy: 12th Australasian Conference, ACISP 2007, Townsville, Australia, July 2-4: Proceedings,* (pp. 171-183) Berlin: Springer. https://doi.org/10.1007/978-3-540-73458-1_14 (Published)

Privacy-preserving credentials upon trusted computing augmented servers, by YANG, Yanjiang; DENG, Robert H.; BAO, Feng. (2007.0). *Information security, practice and experience: 3rd International Conference, ISPEC 2007, Hong Kong, China, May 7-9: Proceedings,* (pp. 177-192) Berlin: Springer. https://doi.org/10.1007/978-3-540-72163-5_15 (Published)

Achieving end-to-end authentication in intermediary-enabled multimedia delivery systems, by DENG, Robert H.; YANG, Yanjiang. (2007.0). *Information security, practice and experience: Third International Conference, ISPEC 2007, Hong Kong, China, May 7-9, Proceedings,* (pp. 284-300) Berlin: Springer. https://doi.org/10.1007/978-3-540-72163-5_22 (Published)

Vulnerability analysis of EMAP: An efficient RFID mutual authentication protocol, by LI, Tieyan; DENG, Robert H.. (2007.0). *2007 2nd International Conference on Availability, Reliability and Security (ARES): Vienna, April 10-13: Proceedings,* (pp. 238-245) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/ARES.2007.159 (Published)

Towards Practical Private Information Retrieval, by DENG, Robert H.. (2006.0). *Proceedings of the International Conference on Information Security and Computer Forensics,* (pp. 253-258) http://www.cs.sunysb.edu/~sion/research/PIR.Panel.Securecomm.2006/giovanni.pdf (Published)

Privacy enhanced superdistribution of layered content with trusted access control, by CHONG, Daniel J. T.; DENG, Robert H.. (2006.0). *DRM '06: Proceedings of the ACM Workshop on Data Warehousing and OLAP, Alexandria, Virginia, October 30,* (pp. 37-44) New York: ACM. https://doi.org/10.1145/1179509.1179517 (Published)

Protecting location information of mobile nodes in Mobile IPv6, by DENG, Robert H.; QIU, Ying; ZHOU, Jianying; BAO, Feng. (2006.0). *First International Conference on Communications and Networking in China, ChinaCom 2006: 25-27 October, Beijing: Proceedings,* (pp. 1-7) Piscataway, NJ: IEEE. https://doi.org/10.1109/CHINACOM.2006.344648 (Published)

An anonymous routing protocol with the local-repair mechanism for mobile ad hoc networks, by ZHU, Bo; JAJODIA, Sushil; KANKANHALLI, Mohan S.; BAO, Feng; DENG, Robert H.. (2006.0). *2006 3rd Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks SECON: Reston, Virginia, 25-28 September: Proceedings,* (pp. 70-79) Piscataway, NJ: IEEE. https://doi.org/10.1109/SAHCN.2006.288411 (Published)

Private Information Retrieval using trusted hardware, by WANG, Shuhong; DING, Xuhua; DENG, Robert H.; BAO, Feng. (2006.0). *Computer Security - ESORICS 2006: 11th European Symposium on Research in Computer Security, Hamburg, Germany, September 18-20: Proceedings,* (pp. 49-64) Berlin: Springer.

https://doi.org/10.1007/11863908_4 (Published)

Practical private data matching deterrent to spoofing attacks, by YANG, Yanjiang; DENG, Robert H.; BAO, Feng. (2006.0). *CIKM '06: Proceedings of ACM 15th Conference on Information and Knowledge Management, Arlington, November 6-11,* (pp. 852-853) New York: ACM. https://doi.org/10.1145/1183614.1183763 (Published)

Rights protection for data cubes, by GUO, Jie; LI, Yingjiu; DENG, Robert H.; CHEN, Kefei. (2006.0). *Information Security: 9th International Conference, ISC 2006, Samos Island, Greece, August 30 - September 2: Proceedings,* (pp. 359-372) Berlin: Springer. https://doi.org/10.1007/11836810_26 (Published)

Practical Inference Control for Data Cubes, by LI, Yingjiu; LU, Haibing; DENG, Robert H.. (2006.0). *IEEE Symposium on Security and Privacy: Proceedings: 21-24 May, 2006, Berkeley/Oakland, California,* (pp. 115-120) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/SP.2006.31 (Published)

Efficient key tree construction for group key agreement in ad hoc networks, by WAN, Zhiguo; ZHU, Bo; DENG, Robert H.; BAO, Feng; ANANDA, A. L.. (2006.0). *2006 IEEE Wireless Communications and Networking Conference: WCNC 2006: 3-6 April, Las Vegas, Nevada,* (pp. 652-658) Piscataway, NJ: IEEE. https://doi.org/10.1109/WCNC.2006.1683546 (Published)

Fortifying password authentication in integrated healthcare delivery systems, by YANG, Yanjiang; DENG, Robert H.; BAO, Feng. (2006.0). *ASIACCS '06: Proceedings of the ACM Symposium on Information, Computer and Communications Security: Taipei, Taiwan, 21-24 March,* (pp. 255-265) New York: ACM. https://doi.org/10.1145/1128817.1128855 (Published)

Publicly verifiable ownership protection for relational databases, by LI, Yingjiu; DENG, Robert H.. (2006.0). *ASIACCS '06: Proceedings of the ACM Symposium on Information, Computer and Communications Security: Taipei, Taiwan, 21-24 March,* (pp. 78-89) New York: ACM. https://doi.org/10.1145/1128817.1128832 (Published)

Cryptanalysis of a forward secure blind signature scheme with provable security, by WANG, Shuhong; BAO, Feng; DENG, Robert H.. (2005.0). *Information and Communications Security: 7th International Conference, ICICS 2005, Beijing, China, December 10-13: Proceedings,* (pp. 53-60) Berlin: Springer. https://doi.org/10.1007/11602897_5 (Published)

Sequential aggregate signatures working over independent homomorphic trapdoor one-way permutation domains, by ZHU, Huafei; BAO, Feng; DENG, Robert H.. (2005.0). *Information and Communications Security: 7th International Conference, ICICS 2005, Beijing, China, December 10-13: Proceedings,* (pp. 207-219) Berlin: Springer. https://doi.org/10.1007/11602897_18 (Published)

Authenticating query results in data publishing, by MA, Di; DENG, Robert H.; PANG, Hwee Hwa; ZHOU, Jianying. (2005.0). *Information and Communications Security: 7th International Conference, ICICS 2005, Beijing, China, December 10-13: Proceedings,* (pp. 376-388) Berlin: Springer. https://doi.org/10.1007/11602897_32 (Published)

A block oriented fingerprinting scheme in relational database, by LIU, Siyuan; WANG, Shuhong; DENG, Robert H.; SHAO, Weizhong. (2004.0). *Information Security and Cryptology - ICISC 2004: 7th International Conference, Seoul, Korea, December 2-3: Revised Selected Papers,* (pp. 455-466) Berlin: Springer. https://doi.org/10.1007/11496618_33 (Published)

Anonymous DoS-Resistant Access Control Protocol using Passwords for Wireless Networks, by WAN, Zhiguo; DENG, Robert H.; BAO, Feng; ANANDA, Akkihebbal L.. (2005.0). *IEEE Conference on Local Computer Networks 30th Anniversary: Proceedings: Sydney, Australia, November 15-17, 2005,* (pp. 328-335) Los Alamitos, CA: IEEE Computer Society. http://dx.doi.org/10.1109/LCN.2005.30 (Published)

On security notions of steganographic systems, by CHANG, Kisik; DENG, Robert H.; BAO, Feng; LEE, Sangjin; KIM, Hyungjun. (2005.0). *Digital Watermarking: Third International Workshop, IWDW 2004, Seoul, South Korea, October 30 - November 1: Revised Selected Papers,* (pp. 137-151) Berlin: Springer. https://doi.org/10.1007/978-3-540-31805-7_12 (Published)

Protocol for hiding movement of mobile nodes in Mobile IPv6, by QIU, Ying; ZHOU, Jianying; BAO, Feng; DENG, Robert H.. (2005.0). *VTC2005-Fall: IEEE 62nd Vehicular Technology Conference, 2005. 25-28 September 2005, Dallas, Texas,* (pp. 812-815) Piscataway, NJ: IEEE. https://doi.org/10.1109/VETECF.2005.1558037 (Published)

Security analysis and improvement of return routability protocol, by QIU, Ying; ZHOU, Jianying; DENG, Robert H.. (2006.0). *Secure Mobile Ad-hoc Networks and Sensors: First International Workshop, MADNES 2005, Singapore, September 20-22, 2005: Revised Selected Papers,* (pp. 174-181) Berlin: Springer. https://doi.org/10.1007/11801412_16 (Published)

An Efficient Certified E-Mail Scheme Suitable for Wireless Mobile Environments, by WANG, Guilin; BAO, Feng; DENG, Robert H.. (2005.0). *PIMRC 2005: Proceedings of the 16th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications, Berlin, Germany, September 11-14,* (pp. 1994-1998) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/PIMRC.2005.1651789 (Published)

How much you watch, how much you pay, by WU, Yongdong; PANG, Hwee Hwa; DENG, Robert H.. (2005.0). *SPIE Proceedings: Visual Communications and Image Processing Conference 2005, July 12-15, Beijing, China,* (pp. 961-968) Bellingham, WA: SPIE. https://doi.org/10.1117/12.632558 (Published)

Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults, by BAO, F.; DENG, Robert H.; HAN, Y.; JENG, A.; NARASIMHALU, A. D.; NGAIR, T.. (2005.0). *5th International Workshop: Proceedings International Workshop on Security Protocols, Paris, France, 1997 April 7–9,* (pp. 115-124) Paris, France: Springer. http://doi.org/10.1007/BFb0028164 (Published)

Secure human communications based on biometrics signals, by WU, Yongdong; BAO, Feng; DENG, Robert H.. (2005.0). *Security and Privacy in the Age of Ubiquitous Computing: IFIP TC11 20th International Information Security Conference May 30-June 1, Chiba, Japan,* (pp. 95-111) Berline: Springer. https://doi.org/10.1007/0-387-25660-1_14 (Published)

A new architecture for user authentication and key exchange using password for federated enterprises, by YANG, Yanjiang; BAO, Feng; DENG, Robert H.. (2005.0). *Security and Privacy in the Age of Ubiquitous Computing: IFIP TC11 20th International Information Security Conference May 30-June 1, Chiba, Japan,* (pp. 95-111) Berlin: Springer. https://doi.org/10.1007/0-387-25660-1_7 (Published)

Protecting group dynamic information in large scale multicast groups, by WU, Yongdong; LI, Tieyan; DENG, Robert H.. (2005.0). *Security and Privacy in the Age of Ubiquitous Computing: IFIP TC11 20th International Information Security Conference May 30-June 1, Chiba, Japan,* (pp. 459-475) Berlin: Springer. https://doi.org/10.1007/0-387-25660-1_30 (Published)

Providing efficient certification services against active attacks in ad hoc networks, by ZHU, Bo; WANG, Guilin; WAN, Zhiguo; KANKANHALLI, Mohan S.; BAO, Feng; DENG, Robert H.. (2005.0). *2005 IEEE International Performance, Computing, and Communications Conference: IPCCC, Phoenix, AZ, April 7-9, Proceedings,* (pp. 285-292) Piscataway, NJ: IEEE. https://doi.org/10.1109/PCCC.2005.1460571 (Published)

Privacy and ownership preserving of outsourced medical data, by BERTINO, Elisa; OOI, Beng Chin; YANG, Yanjiang; DENG, Robert H.. (2005.0). *ICDE 2005: 21st International Conference on Data Engineering, 5-8 April, Tokyo, Japan: Proceedings,* (pp. 521-532) Los Alamitos, CA: IEEE Computer Society. https://doi.org/10.1109/ICDE.2005.111 (Published)

DoS-resistant access control protocol with identity confidentiality for wireless networks, by WAN, Zhiguo; ZHU, Bo; DENG, Robert H.; BAO, Feng; ANANDA, A. L.. (2005.0). *WCNC 2005: IEEE Wireless Communications and Networking Conference: Broadband Wireless for the Masses: Ready for Take-off, 13-17 March, New Orleans, LA,* (pp. 1521-1526) Piscataway, NJ: IEEE. https://doi.org/10.1109/WCNC.2005.1424740 (Published)

On security notions for steganalysis (Extended abstract), by CHANG, Kisik; DENG, Robert H.; BAO, Feng; LEE, Sangjin; KIM, Hyungjun; LIM, Jongin. (2004.0). *Information Security and Cryptology ICISC 2004: 7th International Conference, Seoul, Korea, December 2-3: Revised Selected Papers,* (pp. 440-454) Berlin: Springer. https://doi.org/10.1007/11496618_32 (Published)

Anonymous Secure Routing in Mobile Ad-Hoc Networks, by ZHU, Bo; WAN, Zhiguo; Kankanhalli, Mohan S.; BAO, Feng; DENG, Robert H.. (2004.0). *LCN 2004: 29th Annual IEEE International Conference on Local Computer Networks: Proceedings: Tampa, Florida, November 16-18, 2004,* (pp. 102-108) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/LCN.2004.21 (Published)

Flexible verification of MPEG-4 stream in peer-to-peer CDN, by LI, Tieyan; WU, Yongdong; MA, Di; DENG, Robert H.. (2004.0). *Information and Communications Security: 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29: Proceedings,* (pp. 79-91) Berlin: Springer. https://doi.org/10.1007/978-3-540-30191-2_7 (Published)

Dynamic access control for multi-privileged group communications, by MA, Di; DENG, Robert H.; WU,

Yongdong; LI, Tieyan. (2004.0). *Information and Communications Security: 6th International Conference, ICICS 2004, Malaga, Spain, October 27-29: Proceedings,* (pp. 508-519) Berlin: Springer. https://doi.org/10.1007/978-3-540-30191-2_39 (Published)

Progressive protection of JPEG2000 codestreams, by WU, Yongdong; MA, Di; DENG, Robert H.. (2004.0). *ICIP 2004: IEEE International Conference on Image Processing: 24-27 October, 2004, Singapore: Proceedings,* (pp. 3447-3450) Piscataway, NJ: IEEE. https://doi.org/10.1109/ICIP.2004.1421856 (Published)

Compliant encryption of JPEG2000 codestreams, by WU, Yongdong; DENG, Robert H.. (2004.0). *2004 International Conference on Image Processing ICIP: 24-27 October, Singapore: Proceedings,* (pp. 3439-3442) Piscataway, NJ: IEEE. https://doi.org/10.1109/ICIP.2004.1421854 (Published)

Trust establishment in large scale grid settings, by ZHU, Bo; LI, Tieyan; ZHU, Huafei; KANKANHALLI, Mohan S.; BAO, Feng; DENG, Robert H.. (2004.0). *Grid and Cooperative Computing - GCC 2004: Third International Conference, Wuhan, China, October 21-24: Proceedings,* (pp. 317-324) Berlin: Springer. https://doi.org/10.1007/978-3-540-30208-7_46 (Published)

Security analysis of two signcryption schemes, by WANG, Guilin; DENG, Robert H.; KWAK, DongJin; MOON, Sangjae. (2004.0). *Information Security: 7th International Conference, ISC 2004, Palo Alto, CA, September 27-29: Proceedings,* (pp. 123-133) Berlin: Springer. https://doi.org/10.1007/978-3-540-30144-8_11 (Published)

Proxy signature scheme with multiple original signers for wireless e-commerce applications, by WANG, Guilin; BAO, Feng; ZHOU, Jianying; DENG, Robert H.. (2004.0). *Proceedings of the 2004 IEEE 60th Vehicular Technology Conference: 26-29 September, Los Angeles, CA,* (pp. 3249-3253) Piscataway, NJ: IEEE. https://doi.org/10.1109/VETECF.2004.1404663 (Published)

Computing of trust in wireless networks, by ZHU, Huafei; BAO, Feng; DENG, Robert H.. (2004.0). *Proceedings of the 60th IEEE Vehicular Technology Conference: 26-29 September 2004, Los Angeles,* (pp. 2621-2624) Piscataway, NJ: IEEE. https://doi.org/10.1109/VETECF.2004.1400531 (Published)

Classify Encrypted Data in Wireless Sensor Networks, by WU, Yongdong; MA, Di; LI, Tieyan; DENG, Robert H.. (2004.0). *Proceedings of the 2004 IEEE 60th Vehicular Technology Conference, 26-29 September, Los Angeles, California,* (pp. 3236-3239) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/VETECF.2004.1404660 (Published)

Securing return routability protocol against active attack, by ZHU, Huafei; BAO, Feng; DENG, Robert H.. (2004.0). *Proceedings of the 60th IEEE Vehicular Technology Conference, 26-29 September 2004, Los Angeles, CA,* (pp. 3254-3257) Piscataway, NJ: IEEE. https://doi.org/10.1109/VETECF.2004.1404664 (Published)

On the security of the Lee-Hwang group-oriented undeniable signature schemes, by WANG, Guilin; ZHOU, Jianying; DENG, Robert H.. (2004.0). *Trust and Privacy in Digital Business: First International Conference, TrustBus 2004, Zaragoza, Spain, August 30 - September 1: Proceedings,* (pp. 289-298) Berlin: Springer. https://doi.org/10.1007/978-3-540-30079-3_30 (Published)

Packet-loss resilient coding scheme with only XOR operations, by FENG, Gui Liang; DENG, Robert H.; BAO, Feng. (2004.0). *IEE Proceedings: Communications,* (pp. 322-328) London: IEE. https://doi.org/10.1049/ip-com:20040423 (Published)

Cryptanalysis of two anonymous buyer-seller watermarking protocols and an improvement for true anonymity, by GOI, Bok-Min; PHAN, Raphael C. W.; YANG, Yanjiang; BAO, Feng; DENG, Robert H.; SIDDIQI, M. U.. (2004.0). *Applied Cryptography and Network Security: Second International Conference, ACNS 2004, Yellow Mountain, China, June 8-11, 2004: Proceedings,* (pp. 369-382) Berlin: Springer. https://doi.org/10.1007/978-3-540-24852-1_27 (Published)

A secure and privacy enhanced Location-Based Service transaction protocol in ubiquitous computing environment, by DIVYAN, Konidala; DENG, Robert H.; ZHOU, Jianying; KIM, Kwanjo. (2004.0). *SCIS 2004: Proceedings of the 2004 Symposium on Cryptography and Information Security, Sendai, 27-30 January,* (pp. 931-936) Tokyo: IEICE. (Published)

An Improved Personal CA for Personal Area Networks, by DENG, Robert H.; BAO, Feng. (2003.0). *GLOBECOM '03: IEEE Global Telecommunications Conference: 1-5 December, 2003, San Francisco,* (pp. 1468-1490) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/GLOCOM.2003.1258485 (Published)

Security analysis of some proxy signatures, by WANG, Guilin; BAO, Feng; ZHOU, Jianying; DENG, Robert H..

(2004.0). *Information Security and Cryptology - ICISC 2003: 6th International Conference, Seoul, Korea, November 27-28: Revised Papers,* (pp. 305-319) Berlin: Springer. https://doi.org/10.1007/978-3-540-24691-6_23 (Published)

A Flexible and Scalable Authentication Scheme for JPEG 2000 Image Codestreams, by PENG, Cheng; DENG, Robert H.; WU, Yongdong; SHAO, Weizhong. (2003.0). *MM'03: Proceedings of the 11th ACM International Conference on Multimedia, Berkeley, CA, November 4-6, 2003,* (pp. 441-443) New York: ACM. http://dx.doi.org/10.1145/957013.957101 (Published)

Variations of Diffie-Hellman problem, by BAO, Feng; DENG, Robert H.; ZHU, Huafei. (2003.0). *Information and Communications Security: 5th International Conference, ICICS 2003, Huhehaote, China, October 10-13, Proceedings,* (pp. 301-312) Berlin: Springer. https://doi.org/10.1007/978-3-540-39927-8_28 (Published)

Making the key agreement protocol in mobile ad hoc network more efficient, by YAO, Gang; REN, Kui; BAO, Feng; DENG, Robert H.; FENG, Dengguo. (2003.0). *Applied Cryptography and Network Security: First International Conference, ACNS 2003, Kunming, China, October 16-19: Proceedings,* (pp. 343-356) Berlin: Springer. https://doi.org/10.1007/978-3-540-45203-4_27 (Published)

Security remarks on a group signature scheme with member deletion, by WANG, Guilin; BAO, Feng; ZHOU, Jianying; DENG, Robert H.. (2003.0). *Information and Communications Security: 5th International Conference, ICICS 2003, Huhehaote, China, October 10-13: Proceedings,* (pp. 72-83) Berlin: Springer. https://doi.org/10.1007/978-3-540-39927-8_7 (Published)

Adaptive collusion attack to a block oriented watermarking scheme, by WU, Yongdong; DENG, Robert H.. (2003.0). *Information and Communications Security: 5th International Conference, ICICS 2003, Huhehaote, China, October 10-13,* (pp. 238-248) Berlin: Springer. https://doi.org/10.1007/978-3-540-39927-8_22 (Published)

An efficient known plaintext attack on FEA-M, by WU, Hongjun; BAO, Feng; DENG, Robert H.. (2003.0). *Information and Communications Security: 5th International Conference, ICICS 2003, Huhehaote, China, October 10-13: Proceedings,* (pp. 84-87) Berlin: Springer. https://doi.org/10.1007/978-3-540-39927-8_8 (Published)

An efficient public-key framework, by ZHOU, Jianying; BAO, Feng; DENG, Robert H.. (2003.0). *Information and Communications Security: 5th International Conference, ICICS 2003, Huhehaote, China, October 10-13: Proceedings,* (pp. 88-99) Berlin: Springer. https://doi.org/10.1007/978-3-540-39927-8_9 (Published)

Validating digital signatures without TTP's time-stamping and certificate revocation, by ZHOU, Jianying; BAO, Feng; DENG, Robert H.. (2003.0). *Information Security: 6th International Conference, ISC 2003, Bristol, UK, October 1-3: Proceedings,* (pp. 96-110) Berlin: Springer. https://doi.org/10.1007/10958513_8 (Published)

Flexible authentication of images, by YANG, Yanjiang; BAO, Feng; DENG, Robert H.. (2003.0). *Proceedings of SPIE: Visual Communications and Image Processing 2003: 8-11 July 2003, Lugano, Switzerland,* (pp. 1905-1911) Bellingham, WA: SPIE. http://dx.doi.org/10.1117/12.503075 (Published)

Secure the image-based simulated telesurgery system, by YANG, Yanjiang; WANG, Zhelan; BAO, Feng; DENG, Robert H.. (2003.0). *ISCAS 2003: Proceedings of the IEEE International Symposium on Circuits and Systems, May 25-28, Bangkok, Thailand,* (pp. 596-599) Piscataway, NJ: IEEE. http://dx.doi.org/10.1109/ISCAS.2003.1206044 (Published)

Defending against redirect attacks in mobile IP, by DENG, Robert H.; ZHOU, Jianying; BAO, Feng. (2002.0). *CCS '02: Proceedings of the 9th ACM Conference on Computer and Communications Security, November 18-22, Washington, DC,* (pp. 59-67) New York: ACM. http://dx.doi.org/10.1145/586110.586120 (Published)

Cryptanalysis of some hash functions based on block ciphers and codes, by WU, Hongjun; BAO, Feng; DENG, Robert H.. (2002.0). *2002 International Workshop on Cryptology and Network Security, 26-28 September, San Francisco, CA,* (pp. 221-224) San Francisco, CA: (Published)

Security analysis and improvement of the global key recovery system, by YANG, Yanjiang; BAO, Feng; DENG, Robert H.. (2002.0). *Information Security and Privacy: 7th Australasian Conference, ACISP 2002 Melbourne, Australia, July 3-5, 2002: Proceedings,* (pp. 17-24) Berlin: Springer. https://doi.org/10.1007/3-540-45450-0_2 (Published)

Privacy protection for transactions of digital goods, by BAO, Feng; DENG, Robert H.. (2001.0). *Information*

*and Communications Security: Third International Conference, ICICS 2001: Xian, China, November 13-16, Proceedings,* (pp. 202-213) Berlin: Springer. https://doi.org/10.1007/3-540-45600-7_23 (Published)

Design of portable mobile devices based e-payment system and e-ticketing system with digital signature, by BAO, Feng; Anantharaman, L.; DENG, Robert H.. (2001.0). *International conferences on Info-tech and Info-net: Proceedings: ICCII 2001-Beijing, October 29-November 1, 2001, Beijing, China,* (pp. 7-13) Beijing, China: IEEE. http://dx.doi.org/10.1109/ICII.2001.982996 (Published)

Secure and private distribution of online video and some related cryptographic issues, by BAO, Feng; DENG, Robert H.; BAO, Peirong; GUO, Yan; WU, Hongjun. (2001.0). *Information Security and Privacy: 6th Australasian Conference, ACISP 2001 Sydney, Australia, July 11-13: Proceedings,* (pp. 190-205) Berlin: Springer. https://doi.org/10.1007/3-540-47719-5_17 (Published)

An optical watermarking solution for authenticating printed document, by SUN, Q. B.; FENG, P. R.; DENG, Robert H.. (2001.0). *Proceedings of the International Conference on Information Technology: Coding and Computing, 2-4 April 2001, Las Vegas, Nevada,* (pp. 65-70) Los Alamitos, CA: IEEE Computer Society. http://dx.doi.org/10.1109/ITCC.2001.918767 (Published)

Cryptanalysis of two sparse polynomial based public key cryptosystems, by BAO, Feng; DENG, Robert H.; Geiselmann, Willi; Schnorr, Claus; Steinwandt, Rainer; Wu, Hongjun. (2001.0). *Public Key Cryptography: 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001 Cheju Island, Korea, February 13-15: Proceedings,* (pp. 153-164) Berlin: Springer. https://doi.org/10.1007/3-540-44586-2_11 (Published)

Cryptanalysis of a digital signature scheme on ID-based key-sharing infrastructures, by WU, Hongjun; BAO, Feng; DENG, Robert H.. (2001.0). *Public Key Cryptography: 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001, Cheju Island, Korea, February 13-15: Proceedings,* (pp. 173-179) Berlin: Springer. https://doi.org/10.1007/3-540-44586-2_13 (Published)

An efficient and practical scheme for privacy protection in e-commerce of digital goods, by BAO, Feng; DENG, Robert H.; FENG, Peirong. (2000.0). *Information Security and Cryptology - ICISC 2000: Third International Conference, Seoul, Korea, December 8-9: Proceedings,* (pp. 162-170) Berlin: Springer. https://doi.org/10.1007/3-540-45247-8_13 (Published)

Electronic payment systems with fair on-line verification, by BAO, Feng; DENG, Robert H.; ZHOU, Jianying. (2000.0). *Information Security for Global Information Infrastructures: IFIP TC11 Sixteenth Annual Working Conference on Information Security August 22-24, 2000, Beijing, China,* (pp. 451-460) Berlin: Springer. https://doi.org/10.1007/978-0-387-35515-3_46 (Published)

Cryptanalysis of polynomial authentication and signature scheme, by WU, Hongjun; BAO, Feng; YE, Dingfeng; DENG, Robert H.. (2000.0). *Information Security and Privacy: 5th Australasian Conference, ACISP 2000, Brisbane, Australia, July 10-12: Proceedings,* (pp. 278-288) Berlin: Springer. https://doi.org/10.1007/10718964_23 (Published)

Cryptanalysis of the m-permutation protection schemes, by WU, Hongjun; BAO, Feng; YE, Dingfeng; DENG, Robert H.. (2000.0). *Information Security and Privacy: 5th Australasian Conference, ACISP 2000, Brisbane, Australia, July 10-12, Proceedings,* (pp. 97-111) Berlin: Springer. https://doi.org/10.1007/10718964_9 (Published)

Some remarks on a fair exchange protocol, by ZHOU, Jianying; DENG, Robert H.; BAO, Feng. (2000.0). *Public Key Cryptography: Third International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2000, Melbourne, Victoria, Australia, January 18-20,* (pp. 46-57) Berlin: Springer. https://doi.org/10.1007/978-3-540-46588-1_4 (Published)

Proactive Secret Sharing schemes with different security levels, by BAO, Feng; DENG, Robert H.. (2000.0). *Proceedings of ChinaCrypt 2000,* (pp. 92-101) Beijing: Science Press. https://worldcat.org/isbn/9787030082626 (Published)

A Ubiquitous Secure and Reliable Digital Data Depository System, by DENG, Robert H.; FENG, Jian; BAO, Feng; NARASIMHALU, Arcot Desai. (1998.0). *7th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WET ICE '98): June 17-19, 1998, Stanford, California: Proceedings,* (pp. 354-358) Los Alamitos, CA: IEEE Computer Society. http://doi.ieeecomputersociety.org/10.1109/ENABL.1998.725717 (Published)

Efficient and practical fair exchange protocols with off-line TTP, by BAO, Feng; DENG, Robert H.; MAO, Wenbo. (1998.0). *Proceedings of the 1998 IEEE Symposium on Security and Privacy, Oakland, California,*

*May 3-6,* (pp. 77-85) Oakland, USA: IEEE. https://doi.org/10.1109/SECPRI.1998.674825 (Published)

A signcryption scheme with signature directly verifiable by public key, by BAO, Feng; DENG, Robert H.. (1998.0). *Proceedings of the 1st International Workshop on Practice and Theory in Public Key Cryptography: PKC 1998, Yokohama, Japan, February 5-6,* (pp. 55-59) Berlin: Springer. https://doi.org/10.1007/BFb0054014 (Published)

Breaking public key cryptosystems on tamper resistant devices in the presence of transient faults, by BAO, Feng; DENG, Robert H.; HAN, Y.; JENG, A.; NARASIMHALU, Arcot Desai; NGAIR, T.. (1997.0). *Security Protocols: 5th International Workshop: Paris, France, April 7-9, 1997: Proceedings,* (pp. 115-124) Berlin: Springer. https://doi.org/10.1007/BFb0028164 (Published)

A new on-line cash check scheme, by DENG, Robert H.; HAN, Yongfei; JENG, Albert B.; NGAIR, Teow-Hin. (1997.0). *Proceedings of the 4th ACM conference on Computer and communications security, Zurich, Switzerland, 1997 April 1-4,* (pp. 111-116) Zurich, Switzerland: ACM. https://doi.org/10.1145/266420.266444 (Published)

Integrating security in CORBA based object architectures, by DENG, Robert H.; BHONSLE, S. K.; WANG, W.; LAZAR, A. A.. (1995.0). *Proceedings of the 1995 IEEE Symposium on Security and Privacy, Oakland, California, May 8-10,* (pp. 50-61) Oakland, California: IEEE. https://doi.org/10.1109/SECPRI.1995.398922 (Published)

Conference Papers

A comprehensive study for RFID malwares on mobile devices, by YAN, Qiang; LI, Yingjiu; LI, Tieyan; DENG, Robert H.. (2009.0). *Workshop on RFID Security 5th RFIDsec 2009 Asia, January 9-11,* Taipei. (Presented)

Edited Conference Proceedings

*Applied Cryptography and Network Security Workshops: ACNS 2019 Satellite Workshops, SiMLA, Cloud S&P, AIBlock, and AIoTS, Bogota, Colombia, June 5-7: Proceedings,* edited by ZHOU, Jianying; DENG, Robert H.; LI, Zhou; MAJUMDAR, Suryadipta; MENG, Weizhi; WANG, Lingyu; ZHANG, Kehuan. (07/06/2019). Lecture Notes in Computer Science, 11605. Cham: Springer. https://doi.org/10.1007/978-3-030-29729-9 (Published)

*Information security practice and experience,* edited by BAO, Feng; CHEN, Liqun; DENG, Robert H.; WANG, Guojun. (16/11/2016). Lecture Notes in Computer Science, 10060. Zhangjiajie, China: Springer. (Published)

*Security and privacy in communication networks: 12th International Conference, SecureComm 2016, Guangzhou, China, October 10-12, Proceedings,* edited by DENG, Robert H.; WENG, Jian; REN, Kui; YEGNESWARAN, Vinod. (12/10/2016). Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 198. Cham: Springer. https://doi.org/10.1007/978-3-319-59608-2 (Published)

*Information security practice and experience: First International Conference, ISPEC 2005, Singapore, April 11-14: Proceedings,* edited by DENG, Robert H.; BAO, Feng; PANG, Hwee Hwa; ZHOU, Jianying. (11/04/2005). Lecture Notes in Computer Science, 3439. Berlin: Springer. https://doi.org/10.1007/b107167 (Published)

## Research Grants

Singapore Management University

National Satellite of Excellence in Mobile Systems Security and Cloud Security, National Cybersecurity R&D (NCR) Programme, National Research Foundation (NRF) , PI (Project Level): Robert H DENG , Co-PI (Project Level): Debin GAO, PANG Hwee Hwa, DING XuHua, LI Yingjiu, 2019, S$7,498,320

Intelligent and non-instrusive monitoring of Android devices for protection against data-infringing malware, AI Singapore 100 Experiments, AI Singapore , PI (Project Level): Debin GAO , Co-PI (Project Level): David LO, Robert H DENG, 2018, S$479,616

Building next-generation secure environments on smartphones for critical mobile applications, National

Cybersecurity R&D (NCR) Programme, National Research Foundation (NRF) , Co-PI (Project Level): LI Yingjiu, Robert H DENG, 2017, S$1,208,935.08

Deterring Cybersecurity Threats through Internet Topology, Law Enforcement and Technical Mitigation, National Cybersecurity R&D (NCR) Programme, National Research Foundation (NRF) , PI (Project Level): WANG Qiuhong , Co-PI (Project Level): Qian TANG, 2016, S$399,960

Advanced defense techniques for mobile systems and future networks, Huawei Technologies co. Ltd , PI (Project Level): Robert H DENG , Co-PI (Project Level): Debin GAO, DING XuHua, LI Yingjiu, 2015

COMMANDO-HUMANS: COMputational Modelling and Automatic Non-intrusive Detection of HUMan behAviour based iNSecurity, National Cybersecurity R&D (NCR) Programme, National Research Foundation (NRF) , PI (Project Level): Robert H DENG , Co-PI (Project Level): LI Yingjiu, 2015, S$416,021.2

Secure Mobile Centre - Technologies and Solutions for Securing Mobile Computing, National Cybersecurity R&D (NCR) Programme, National Research Foundation (NRF) , PI (Programme Level): Robert H DENG , PI (Project Level): DING XuHua, Debin GAO, JIANG Lingxiao, LI Yingjiu, David LO, PANG Hwee Hwa, 2014, S$6,415,200

Multidimensional Context Awareness Security Techniques, Huawei Technologies co. Ltd , PI (Project Level): Robert H DENG, 2013, S$156,000

Techniques and Systems for Securing Scalable Multimedia Content Dissemination, Public Sector Research Funding (PSF), Agency for Science, Technology and Research (A*STAR) , PI (Project Level): Robert H DENG , Co-PI (Project Level): DING XuHua, 2010, S$605,376

Security Architecture and Techniques for Communications, Control and Management of Energy Distribution Systems, Thematic Strategic Research Program (TSRP), Agency for Science, Technology and Research (A*STAR) , Co-PI (Project Level): Robert H DENG, 2008, S$564,510

A Security Framework for EPCglobal Network (2008), Public Sector Research Funding (PSF), Agency for Science, Technology and Research (A*STAR) , PI (Project Level): LI Yingjiu , Co-PI (Project Level): Robert H DENG, 2008, S$575,640

TeleOph: A Secure Tele-ophthalmology System, The Enterprise Challenge (TEC) Program, The Government of Singapore, Prime Minister's Office , Co-PI (Project Level): Robert H DENG, S$50,200

The Use of Mobile Devices in RFID-Based Supply Chain Management, Nokia (China) Investment Corporation Limited , PI (Project Level): Robert H DENG, S$21,137

Trusted Decentralized Identities, Digital Trust Centre (DTC) Research Grant, National Research Foundation (NRF) , PI (Project Level): YANG Guomin , Co-PI (Project Level): Robert H DENG

Efficient User Credential Revocation in Cloud Computing, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Robert H DENG, 2014, S$41,940.67

Attributed-Based Encryption with Adaptable Security Policies, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Robert H DENG, 2013, S$41,940.67

Privacy-preserving access control of encrypted data in the cloud, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Robert H DENG, 2012, S$39,943.44

Flexible access control of encrypted data in the cloud, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Robert H DENG, 2011, S$37,842

Formal RFID privacy models and protocols, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Robert H DENG, 2010, S$35,677.33

Privacy Protection in RFID-based Business Information Systems, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Robert H DENG, 2009, S$34,462.56

Enforcing data security & privacy in large scale wirless sensor networks using trusted computing technology, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Robert H DENG, 2008, S$33,953.22

End-to-end content authentication in multimedia delivery systems, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Robert H DENG, 2007, S$32,413.56

Inference control and private information retrieval in statistical databases, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Robert H DENG, 2006, S$30,870

Trusted Computing Technology and Its Applications, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Robert H DENG, 2005, S$30,135

Security and trust management in mobile and ad hoc networking, SMU Internal Grant, Ministry of Education (MOE) Tier 1 , PI (Project Level): Robert H DENG, 2004, S$32,400

Other Institutions

IIE(SMART) - sBox - Secure Enterprise Cloud Data Storage System, SMART, Singapore-MIT Alliance for Research and Technology PI (Project Level): Robert H DENG, 2020, SGD250,000

IIE(MDGF) - sBox end-to-end data privacy protection and sharing software system. , MDGF, MOE Decentralised Gap Funding PI (Project Level): Robert H DENG, 2019, SGD250,000

## Intellectual Property

Application/Filed: Robert H DENG, "Method and system for accident avoidance", Singapore Patent 10201406053Q

Application/Filed: Robert H DENG, "R. H. Deng and Y. Li, “Data security system and method for operation thereof”, Singapore patent 10201508390P, PCT Application PCT/SG2016/050132", 24288

Application/Filed: Robert H DENG, "Method and system for correcting eye gaze direction in an image", Singapore Patent 10201503664P

Application/Filed: Robert H DENG, "Data security system and method for operation thereof", Singapore patent 10201508390P

Application/Filed: Robert H DENG, "System and method for determining a security classification of an unknown application", Singapore patent 10201504543V

Granted: Robert H DENG, "Method and apparatus for encrypting and decrypting data", US 7,110,539B1

Granted: Robert H DENG, "Method and apparatus for providing XML document encryption", Singapore Patent 97038

Granted: Robert H DENG, "A method of sale auditing in private transaction of e-goods", PCT WO 03/044619 A2

Granted: Robert H DENG, "Method for cryptographically processing a message", PCT WO2005/034423A1

Granted: Robert H DENG, "Method of generating an authentication", Singapore Patent 110390, US Patent 7,233,782B2

Granted: Robert H DENG, "Method and apparatus for constructing efficient elliptic curve cryptosystems", Singapore 99167 [WO02/0827170]

Granted: Robert H DENG, "Correcting up to two disc drive read errors and detecting the occurrence of more than two read errors ", US Patent 5627843

Granted: Robert H DENG, "Method and apparatus for protecting the legitimacy of an article", UK Patent GB 2364513B

Granted: Robert H DENG, "A method of data storage and apparatus therefor", UK Patent GB 2349964, SG Patent SG 73941

Granted: Robert H DENG, "A method of exchanging digital data", SG Patent SG75691

Granted: Robert H DENG, "Method and apparatus for embedding digital information in digital multimedia data", Singapore Patent 81505, UK Patent GB 2366112, PCT WO00/39954

Granted: Robert H DENG, "A method and apparatus for providing XML document encryption", PCT/SG4

00/00196

Granted: Robert H DENG, "Microprocessor card payment system", SG Patent SG64957

Granted: Robert H DENG, "Method of generating an authentication", US 2005/0246769A

Granted: Robert H DENG, "Method and apparatus for providing XML document encryption", US 2004/0078577A1

Granted: Robert H DENG, "Remote authenticaiton based on exchanging signals representing biometrics information", US Patent 6910129B1

Granted: Robert H DENG, "A public key cryptography and a framework therefore", PCT WO2004/032416A1

Granted: Robert H DENG, "Method for incremental authentication of documents", US 2005/0091261A1

Granted: Robert H DENG, "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", Singapore Patent No. 120791

Granted: Robert H DENG, "Method and apparatus for digital content copy protection", US 6711553B1

Granted: Robert H DENG, "A method of exchanging digital data", European Patent 1082836

Granted: Robert H DENG, "Method and apparatus for encrypting and decrypting data", SG Patent SG 82916

Granted: Robert H DENG, "Legitimacy protection of electronic document and a printed copy thereof", GB 2365184

Granted: Robert H DENG, "Method for incremental authentication of documents", US Patent 7,315,866

Granted: Robert H DENG, "Computationally efficient method for trusted and dynamic digital objects dissemination", US Patent 6058383

### Work in Progress

WANG Qiuhong, Steven MILLER, Robert H DENG, Driving Cybersecurity Policy Insights from Information on the Internet, 2020

## TEACHING

### Courses Taught

Singapore Management University

Postgraduate Professional Programmes :

- Capstone Project - Cybersecurity

Postgraduate Research Programmes :

- Empirical Research Project 1
- Empirical Research Project 4
- Information Security

## THESES AND DISSERTATIONS

### Theses and Dissertations Supervised

Singapore Management University

Supervisor, "Advanced Malware Detection for Android Platform", Dissertation by XU, KE, PhD in Information Systems, Singapore Management University, 2018

Supervisor, "Automatic Vulnerability Detection and Repair", Dissertation by MA SIQI, PhD in Information Systems, Singapore Management University, 2018

Supervisor, "Towards Secure Online Distribution of Multimedia Codestream", Dissertation by LO SWEE WON, PhD in Information Systems, Singapore Management University, 2016

Supervisor, "Virtualization-Based System Hardening
Against Untrusted Kernels", Dissertation by CHENG YUEQIANG, PhD in Information Systems, Singapore Management University, 2014

Supervisor, "Towards Secure and Usable Leakage-Resilient Password Entry", Dissertation by YAN QIANG, PhD in Information Systems, Singapore Management University, 2013

### Theses and Dissertations Assessed

Singapore Management University

Committee Member, "Secure Enforcement Of Isolation Policy On Multicore Platforms With Virtualization Techniques", Dissertation by ZHAO SIQI, PhD in Information Systems, Singapore Management University, 2018

Committee Member, "Techniques for Identifying Mobile Platform Vulnerabilities and Detecting Policy-violating Applications", Dissertation by SU MON KYWE, PhD in Information Systems, Singapore Management University, 2017

Committee Member, "Online Social Network Based Information Disclosure Analysis", Dissertation by LI YAN, PhD in Information Systems, Singapore Management University, 2014

Committee Member, "Security and Privacy in RFID-Enabled Supply Chains", Dissertation by CAI SHAOYING, PhD in Information Systems, Singapore Management University, 2014

Committee Member, "A Study of the Imitation, Collection and Usability Issues of Keystroke Biometrics", Dissertation by TEY CHEE MENG, PhD in Information Systems, Singapore Management University, 2013

Committee Member, "Exploiting Human Factors in User Authentication", Dissertation by GUPTA PAYAS, PhD in Information Systems, Singapore Management University, 2013

## OTHER ACADEMIC AND PROFESSIONAL ACTIVITIES

### Presentation and Talks

Presentations

Keynote, “TEE-assisted crypto systems – towards designing practical data security solutions”, (18 Nov 2023). *25th International Conference on Information and Communications Security (ICICS 2023),*

Keynote, “Hardware-assisted data security & privacy solutions”, (19 Oct 2023). *19th EAI International Conference on Security and Privacy in Communications Networks (SecureComm 2023),*

Keynote, “Data security & privacy protection in IoT MGC systems”, (10 Jul 2023). *The 9th ACM Cyber-Physical System Security Workshop (CPSS 2023),*

Keynote, “Efficiently deployable and efficiently searchable encryption – applications, attacks, and countermeasures”, (18 Dec 2022). ”, *Information Security Conference (ISC 2022),*

Keynote, “Protecting cloud data security and privacy through encryption”, (23 Nov 2022). *17th International Conference on Information Security Practice and Experience (ISPEC 2022),*

10Keynote, “Secure cloud data storage for enterprise users – from cryptographic research to system design”, (15 May 2021). *EAI International Conference on Applied Cryptography in Computer and Communications (AC3 2021),*

Keynote. "Privacy-preserving deep packet inspection on TLS traffic", (25 Nov 2020). *the 14th International Conference on Network and System Security,* Melbourne, Australia.

Keynote, “Towards leakage resilient user authentication", (16 Dec 2019). *15th International Conference on Information Security and Cryptology,* Beijng. China

Keynote, “When seeing is not believing – defeating spoofing attacks in face authentication in mobile platforms”, (06 Dec 2019). *15th International Conference on Information Security and Cryptology,* Nanjing. China

Keynote, “Long road towards secure and usable password authentication”, (18 Nov 2019). *IEEE Conference on Dependable and Secure Computing,* Hangzhou. China

Keynote. Protecting data security and privacy in untrusted servers, (14 Dec 2018). *the 14th International Conference on Information Security and Cryptology (Inscrypt 2018),* Fuzhou.

Keynote. New cryptographic techniques for data security and privacy protection in the cloud, (10 Oct 2018). *Huawei Connect 2018,* Shanghai, China.

Keynote. A user centric and layered approach to mobile security, (25 Sep 2018). *the 14th International Conference on Information Security Practice and Experience (ISPEC 2018),* Tokyo, Japan.

Invited talk. End-to-end secure mobile computing in the Internet of Things, (03 Sep 2018). *the 23rd European Symposium on Research in Computer Security (ESORICS 2018),* Barcelona, Spain.

Keynote. A user centric approach to secure mobile systems and applications, (08 Aug 2018). *the 14th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2018),* Singapore.

Keynote. Strengthening the weakest links in IoT security, (11 Jul 2018). *the 23rd Australasian Conference on Information Security and Privacy (ACISP 2018),*

Keynote. Present and future challenges in IoT security, (19 May 2018). *ACM SIGSAC China Symposium, ACM Turing Celebration Conference (ACM TURC 2018),*

Invited Talk. Present and future challenges in IoT Security, (15 May 2018). *Huawei Strategy and Technology Workshop,*

Keynote. Privacy-preserving access control and computations of encrypted data in the cloud, (13 Dec 2017). *The 10th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS 2017),* Guangzhou. China

Invited talk. A layered approach to secure mobile computing, (27 Jul 2017). *Cyber Week 2017 – Academic Track,* Tel Aviv. Israel

Keynote. Performance and cryptographic key management for mobile users in secure cloud storage systems, (09 Dec 2016). *The 3rd International Symposium on Mobile Security,* Seoul. South Korea

Keynote. Achieving end-to-end security in mobile computing, (06 Jun 2016). *The 21st ACM Symposium on Access Control Models and Technologies,* Shanghai. China

Keynote. Attribute-based encryption for access control of encrypted data in the cloud, (04 Jan 2016). *The 4th International Workshop on Security and Forensics in Cyber Space,* Singapore. Singapore

Invited talk. Achieving data security & privacy in untrusted servers, (17 Dec 2015). *Fudan Science and Innovation Forum,* Shanghai. China

Keynote. Flexible and scalable search and sharing of encrypted data in the cloud, (07 Dec 2015). *The 7th International Conference on Trusted Systems,* Beijing. China

Keynote. Efficient and privacy-preserved sharing of encrypted data in the cloud, (22 Aug 2015). *The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications,* Helsinki. Finland

Distinguished Lecture. Protecting security and privacy of outsourced data in the cloud, (04 Dec 2014). *The Croucher Foundation Advanced Study Institute – Information Security and Privacy in Social Networks and Cloud Computing,* Hong Kong. China

Invited talk. Towards secure and usable user authentication in e-banking and e-payment, (13 May 2014). *2014 Huawei Strategy and Technology Workshop,* Shengzhen. China

Keynote speech. RFID security & privacy –recent developments & challenges, (27 Nov 2013). *The 2013 Workshop on RFID and IoT Security,* Guangzhou. China

Keynote speech. Secure access to outsourced data, (08 May 2013). *The 2013 International Workshop on Security in Cloud Computing,* Hangzhou. China

Keynote speech. Access control of encrypted data in untrusted servers, (12 Dec 2012). *The 4th International Symposium on Cyberspace Safety and Security,* Melbourne. Australia

Keynote Speech. Detecting node clones in wireless sensor networks, (07 Sep 2010). *The 6th International ICST Conference on Security and Privacy in Communication Networks,* Singapore.

Keynote Speech. RFID privacy models and a minimal condition, (12 Dec 2009). *The 5th China International Conference on Information Security and Cryptology,* Beijing.

Keynote Speech. Scalable end-to-end multimedia content authentication techniques, (18 Nov 2009). *The 2009 International Conference on Multimedia Information Networking and Security,* Wuhan. China

Keynote Speech. The future of password, (04 Jun 2009). *The 19th Cryptology and Information Security Conference,* Taipei.

Keynote Speech. Scalable authentication techniques compatible with modern multimedia coding standards, (21 Apr 2008). *The Fourth Information Security Practice and Experience Conference,* Sydney.

Keynote Speech. Towards efficient and novel security solutions - a marriage of crypto and trusted computing platform, (07 May 2007). *The 3rd Information Security Practice and Experience Conference,*

Keynote Speech. Inference control and private information retrieval – two sides of one tapestry, (06 Jun 2006). *The 4th International Conference on Applied Cryptography and Network Security,* Singapore.

Invited Talk. New developments in security systems and cryptographic applications, (11 Dec 2004). *The Croucher Foundation Advanced Study Institute – Cryptography and Wireless Security,* Hong Kong.

Invited Seminars, Talks and Lectures

Bitcoin, blockchain and smart contract, 06 Mar 2018. IT Development Talk to Supreme Court Judges

Privacy enhanced super-distribution of multimedia content, 04 Sep 2004. CyLab Seminar, Pittsburgh, United States of America

## EXTERNAL SERVICE – PROFESSIONAL

Member, Program Committee, IEEE Symposium on Security and Privacy, 1999 (Oakland, CA, USA), 2000 (Oakland, CA, USA).

Member, Program Committee, The 11th Australasian Conference on Information Security and Privacy (ACISP 2006), July 2006, Melbourne, Australia.

Member, Technical Program Committee, IEEE Wireless Networks, Communications and Mobile Computing, IEEE WirelessCom 2005 (June 13-14, 2005, Hawaii, USA)

Member, Program Committee, the 11th European Symposium on Research in Computer Security (ESORICS 2006), September 2006, Hamburg, Germany.

Member, International Advisory Committee, IEEE International Carnahan Conference on Security Technology, 1995 (Sanderstead, Surrey, England), 1997 (Canberra, Australia), 1998 (Alexandria, VA, USA), 1999 (Madrid, Spain).

Member, Program Committee, ACM Symposium on Information, Computer and Communications Security (AsiaCCS 2006), 21-24 March 2006, Taipei, Taiwan, http://www.iis.sinica.edu.tw/asiaccs06/indexhome.html

Member, Program Committee, the 2nd International Conference on Mobile Ad-hoc and Sensor Networks (MSN 2006), December 2006, Hong Kong, China.

Member, Technical Program Committee, IEEE Wireless Communications and Networking Conference 2007 (WCNC 2007), March 2007, Hong Kong, China.

Member, Technical Program Committee, Emerging Networks, Technologies and Standards Symposium, (IEEE WirelessCom 2005), Hawaii, USA, http://sa1.sice.umkc.edu/wc05/

Member, Program Committee, The Second Information Security Practice and Experience Conferecne 2006 (ISPEC 2006), (Hangzhou, China)

Member, Technical Program Committee, Technical Program Committee, The First International Conference on Security and Privacy for Emerging Areas in Communication Networks, SECURECOMM 2005 (5-9 September 2005, Athens, Greece)

Member, Program Committee, Information Security Workshop, 1999 (Kuala Lumpur, Malaysia).

Member, Program Committee, The Seventh International Conference on Electronic Commerce, ICEC 2005, 15-17 Aug 2005, Xi'an, China, http://www.icec2005.org

Chairperson, The 1st Information Security Practice and Experience Conference, 2005 (Singapore)

Member, Program Committee, ChinaCOM 2006, 16-19 October 2006, Beijing, China, http://www.chinacom.org/progcom.html

Member, Technical Program Committee, Workshop on Internet and Network Economics, (WINE 2005), (15-17 December, 2005)

Member, Program Committee, ACM Symposium on Information, Computer and Communications Security (AsiaCCS'2006), (Taipei, Taiwan)

Member, Program Committee, The Seventh International Conference on Information and Communications Security, (ICICS 2005), 10-13 December 2005, Beijing, China, http://www.icics2005.org

Technical Program Committee, Workshop on Mobile, Wireless and Sensor Networks, 2004 (Singapore).

Chairperson, The 8th Information Security Conference 2005 (ISC 2005), 20-23 September 2005,(Singapore)

Member, International Program Committee, the IASTED Conference on Communication, Networks and Security, 2003 (New York, USA).

Member, Technical Program Committee, IEEE Globecom 2005, Symposium on Computer and Networks Security, 2005 (Nov. 28- Dec. 2, 2005, St. Louis, USA).

Member, International Program Committee, The IASTED International Conference on Communication, Network and Information Security (CNIS 2005), (November 14-16 2005, Phoenix, USA)

Member, Program Committee, ACM Conference on Computer and Communications Security, 1999 (Singapore).

Member, Technical Program Committee, The 1st IEEE Workshop on Information Assurance in Wireless Sensor Networks 2005 (WSNIA 2005), (April 7-9, Arizona, USA)

Member, Program Committee, Program Committee, ACM Workshop on Digital Rights Management (ACM DRM 2006), October 2006, Washington, DC, USA.

Member, Technical Program Committee, IFIP International Conference on Embedded and Ubiquitous Computing (EUC 2007), December 2007, Taipei, Taiwan.

Member, International Program Committee, IASTED International Conference on Communications and Computer Networks, CCN'2005 (Oct. 24-26, 2005, Marina Del Rey, CA, USA)

Member, Program Committee, the First International Conference on Applied Cryptography and Network Security, 2003 (Kuming, China), 2006 (Singapore)

Member, Program Committee, the Annual International Conference on Information Security and Cryptology, 2003 (Seoul, Korea), 2004 (Seoul, Korea).

Member, Technical Program Committee, The Second International Conference on Security and Privacy for Emerging Areas in Communication Networks (SECURECOMM 2006), September 2006, Baltimore, USA.

Member, Program Committee, Asiacrypt 2003 (Taipei, Taiwan).

Member, Program Committee, the 12th European Symposium on Research in Computer Security (ESORICS 2007), September 2007, Dresden, Germany.

Member, Program Committee, ChinaCOM 2006, October 2006, Beijing, China.

Member, Program Committee, International Conference on Information and Communications Security, 1997 (Beijing, China), 1999 (Sydney, Australia), 2003 (Huhehote, China), 2004 (Malaga, Spain), 2005 (Beijing, China).

Chairperson, Program Committee, The First Conference on Availability, Reliability and Security (AReS 2006), 20th-22nd April 2006, Vienna, Austria.

Member, Technical Program Committee, IEEE Globecom 2003, Symposium on Communications Security, 2003 (San Francisco, USA).

Chairperson, Program Committee, International Public Key Cryptosystems Workshop, 2004 (Singapore)

Member, Advisory Committee, the 1st International Conference on Information Security and Computer Forensics (ISCF 2006), December 2006, Chennai, India.

Member, Program Committee, the 11th European Symposium on Research in Computer Security (ESORICS 2006), 18-20 September 2006, Hamburg, Germany, http://www.esorics06.tu-harburg.de

Chairperson, Program Committee, the International Conference on Information and Communications Security, 2002 (Singapore).

Member, Program Committee, the Second International Workshop for Asian Public Key Infrastructures, 2002 (Taipei, Taiwan).

Member, Program Committee, The Second Conference on Availability, Reliability and Security (AReS 2007), 10th-13th April 2007, Vienna, Austria.

Member, Program Committee, The Third Australasian Information Security Workshop (AISW 2005): Digital Rights Management, 31 Jan - 3 Feb 2005 (Australia)

Member, Program Committee, the 11th Australasian Conference on Information Security and Privacy (ACISP 2006), 3-5 July 2006, Melbourne, Australia, http://acisp2006.it.deakin.edu.au

Member, Technical Program Committee, The IEEE Communications Society/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks, (SECURECOMM 2006), 11-15 September 2006, Baltimore, USA, http://www.securecomm.org

Member, Program Committee, International Conference on Applied Cryptography and Network Security (ACNS 2006), June 2006, Singapore.

Member, Program Committee, ACM Conference on Computer and Communications Security, (ACM CCS 2007), October 2007, Washington, DC, USA.

Member, Program Committee, IEEE Conference on Availability, Reliability and Security (AReS 2006), 20-22 April 2006, Vienna, Austria, http://www.ares-conf.org

Member, Program Committee, the Fourth International Conference on Applied Cryptography and Network Security (ANCS 2006), 6-9 June, Singapore, http://acns2006.i2r.a-star.edu.sg

Member, Technical Program Committee, IEEE International Conference on Communications (ICC 2006) - Wireless Ad Hoc and Sensor Networks, 11th - 15th June 2006, Istanbul, Turkey, http://www.icc2006.org/index.html

Committee Chair, Program Committee, 2021 IEEE Conference on Dependable and Secure Computing, 2021

Committee Chair, Program Committee, 2020 Information Security Conference, 2020

Guest Editor, Special Issue on FinTech Security and Privacy, Future Generation Computer Systems, 2020 - Present

Guest Editor, Special Issue on security and privacy of blockchain technologies, International Information Security, 2020 - Present

Member Board of Advisors, Information Security and Cryptography book series, Springer Verlag's, 2020 - Present

Editor Associate Editor, ACM Transactions on Privacy and Security (TOPS), 2020 - Present

Committee Chair, Program Committee, International Conference on Cryptology and Network Security (CANS), 2019

Editor Book, 3rd Edition of Encyclopedia of Cryptography, Security and Privacy, Springer, 2019 - 2020

Committee Chair, Program Committee, International Conference on Applied Cryptography and Network Security (ACNS), 2019

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, 2017

Committee Member, Steering Committee, ACM Symposium on Access Control Models and Technologies, 2017 - 2020

Guest Editor, Special Issue on Cryptography and Data Security in Cloud Computing, Information Sciences, Elsevier, Vol. 387, May 2017, 2017

Committee Member, Steering Committee, IEEE Conference on Dependable and Secure Computing, 2017 - Present

Editorial Board, SpringerBriefs in Cyber Security Systems and Networks, 2017 - Present

Chairperson, Program Committee, Information Security Practice and Experience Conference (ISPEC), 2016

Chairperson, 12th EAI International Conference on Security and Privacy in Communication Networks (SecureComm), 2016

Editor Associate Editor, IEEE Security and Privacy Magazine, 2016 - 2020

Chairperson, Information Security Practice and Experience Conference (ISPEC), 2015

Chairperson, Information Security Practice and Experience Conference (ISPEC), 2014

Chairperson, Program Committee, International Symposium on Cyberspace Safety and Security, 2014

Member, Program committee, The ACM Cloud Computing Security Workshop, 2014

Guest Editor, Special Issue on Security and Privacy of Electronic Health Information Systems, International Journal of Information Security, Vol. 14, No. 6, November 2015, 2014 - 2015

Member, Program Committee, International Symposium on Cyberspace Safety and Security, 2013

Chairperson, Program Committee, 9th Information Security Practice and Experience Conference., 2013

Member, Program Committee, 2013 iConference, 2013

Editorial Board Member, Special Issue on Security and Privacy in Complex Systems, IEEE Systems Journal, 2013 - 2014

Chairperson, Steering Committee, ACM Symposium on Information, Computer and Communications Security (AsiaCCS), 2013 - 2017

Editorial Board Member, International Journal of Information Security, Springer, 2013 - Present

Member, International Advisory Committee, IEEE Conference on Communications and Network Security, 2013 - Present

Guest Editor, Special Issues on Turst in Cyber, Physical and Social Computing, Computer & Security, Vol. 47, November 2014, 2013 - 2014

Member, International Advisory Committee, International Conference on Network and System Security, 2013 - Present

Guest Editor, Special Issue on Cryptography in Cloud Computing., Future Generation Computer Systems, Vol. 30, January 2014., 2013 - 2014

Member, Program Committee, The 6th International Conference on Network and System Security, 2012

Member, Program Committee, The 19th ACM Conference on Computer and Communications Security., 2012

Chairperson, Program Committee, Information Security Practice and Experience Conference, 2012

Member, Program Committee, International Conference on Applied Cryptography and Network Security, 2012

Member, Program Committee, The Sixth International Conference on Software Security and Reliability., 2012

Member, Program Committee, The Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks., 2012

Chairperson, Technical Proogram Committee, International Conference on Multimedia Information Networking and Security., 2012

Member, Program Committee, ACM Symposium on Information, Computer and Communications Security, 2012

Editor Associate Editor, Associate Editor, IEEE Transactions on Dependable and Secure Computing, 2012 - 2016

Committee Member, Steering Committee, International Conference on Network and System Security, 2012 - Present

Member, Program Committee, ACM Multimedia Conference, 2011

Chairperson, Program Committee, International Conference on Trusted Systems, 2011

Member, Program Committee, IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2011

Member, Program Committee, ACM Conference on Wireless Network Security, 2011

Chairperson, Program Committee, Information Security Practice and Experience Conference, 2011

Member, Program Committee, ACM Symposium on Information, Computer and Communications Security, 2011

Other, Guest Editor, Special Issue on Ubiquitous Electronic Commerce Systems, Journal of Electronic Commerce Research, Vol. 11, No. 1, 2011, Springer,, 2011

Chairperson, Program Committee, International Conference on Trusted Systems, 2010

Chairperson, Program Committee, Information Security Practice and Experience Conference, 2010

Member, Program Committee, International Conference on Information Security and Cryptology, 2010

Member, Program Committee, International Conference on Trusted Cloud Infrastructure TechnologiesAnnual, 2010

Member Board of Advisors, International Advisory Board, International Workshop on Multimedia, Information Privacy and Intelligent Computing Systems, 2010

Member, Program Committee, International Symposium on Data, Privacy and E-Commerce, 2010

Member, Program Committee, IEEE International Conference on Secure Software Integration and Reliability Improvement, 2010

Member, Program Committee, International Conference on Applied Cryptography and Network Security, 2010

Member, Program Committee, International Conference on Applied Cryptography and Network Security, 2010

Member, Program Committee, ACM Symposium on Information, Computer and Communications Security, 2010

Chairperson, Technical Committee, International Conference on Multimedia Information Networking and Security, 2010

Member, Program Committee, ACM Workshop on Scalable Trusted Computing, 2010

Chairperson, Program Committee, The International Conference on Trusted Systems, 2009

Member, Program Committee, International Conference on Information Security and Cryptology, 2009

Member, Technical Program Committee, International Conference on Multimedia Information Networking and Security, 2009

Member, Program Committee, International Conference on Network and System Security, 2009

Member, International Advisory Board, International Workshop on Multimedia, Information Privacy and Intelligent Computing Systems, 2009

Member, Program Committee, ACM Symposium on Information, Computer and Communications Security, 2009

Member, Program Committee, International Conference on the Technical and Socio-economic Aspects of Trusted Computing, 2009

Member, Program Committee, IEEE International Symposium on Trust, Security and Privacy for Pervasive Applications, 2009

Chairperson, Program Committee, Information Security Practice and Experience Conference, 2009

Member, Program Committee, Australasian Conference on Information Security and Privacy, 2009

Member, Program Committee, International Conference on Cloud Computing, 2009

Other, Associate Editor, IEEE Transactions on Information Forensics and Security (since March 2009), 2009 - 2011

Member, Editorial Board, International Journal of Multimedia Intelligence and Security, Inderscience, 2009 - 2017

Member, Technical Program Committee, IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, 2008

Member, Program Committee, International Conference on Computational Intelligence and Security, 2008

Member, Program Committee, International Conference on Information and Communications Security, 2008

Member, Program Committee, International Conference on Network and System Security, 2008

Member, Program Committee, Information Security Conference, 2008

Member, Program Committee, International Conference on Communications and Networking in China, 2008

Member, Program Committee, Annual Computer Security Applications Conference, 2008

Member, Program Committee, Asia Pacific Trusted Infrastructure Technologies Conference, 2008

Member, Technical Program Committee, IEEE International Conference on Communications, 2008

Member, Program Committee, ACM Symposium on Information, Computer and Communications Security, 2008

Member, Program Committee, International Conference on Cryptology and Network Security, 2008

Member, Program Committee, International Conference on Provable Security, 2008

Member, Program Committee, Annual Conference on Privacy, Security and Trust, 2008

Committee Chair, Program Committee, ACM Conference on Computer and Communications Security, 2007

Editor Associate Editor, Security and Communication Network Journal, John Wiley and Sons, 2007 - 2013

Other, Editorial Board, Journal of Computer Science and Technology (JCST), Institute of Computing Technology, Chinese Academy of Sciences, co-publisshed by Springer (2006-), 2006 - Present

Other, Editorial Board, Advances in Cryptology and Information Security (ACSI) series, IOS Press (since August 2005), 2005 - Present

## EXTERNAL SERVICE – PUBLIC SECTOR AND COMMUNITY SERVICE

Committee Chair, Trust Tech Technical Committee , Digital Trust Centre, IMDA, 2022 - 2027

Member, National Cybersecurity R&D Technical Review Panel , CSA, 2022 - 2027