

ACISP 2018 Program

Location: University of Wollongong, Building 20, Ground Floor

Talk time: full paper - 25 mins; short paper - 15 mins

2018-07-11 (Wednesday)

08:00-17:25	Registration	
09:00-09:30 Room 20-3	Opening <i>Prof. Valerie Linton</i>	
09:30 – 10:30 Room 20-3	Keynote (Chair: Willy Susilo) <i>Strengthening the weakest links in IoT Security</i> <i>Prof. Robert H. Deng</i>	
10:30 – 10:50	Coffee Break	
10:50 – 12:30 Room 20-3	Session 1: Blockchain and Cryptocurrency (Chair: TBA) Decentralized Blacklistable Anonymous Credentials with Reputation Rupeng Yang, Man Ho Au, Qiuliang Xu and Zuoxia Yu Z-Channel: Scalable and Efficient Scheme in Zerocash Yuncong Zhang, Yu Long, Zhen Liu, Zhiqiang Liu and Dawu Gu Fast Lottery-based Micropayments for Decentralized Currencies Kexin Hu and Zhenfeng Zhang Revisiting the Incentive Mechanism of Bitcoin-NG Jiayuan Yin, Changren Wang, Zongyang Zhang and Jianwei Liu	
12:30 – 13:30	Lunch	
13:30 – 14:30 Room 20-3	Jennifer Seberry Lecture (Chair: Jennifer Seberry) <i>Location Privacy and its Applications</i> <i>Prof. Wanlei Zhou</i>	
14:35 – 15:50 Session 2A: Room 20-3	Session 2A: Post-quantum Cryptography (I) Chair (TBA) Efficient Decryption Algorithms for EFC Type Encryption Schemes Yacheng Wang, Yasuhiko Ikematsu, Dung Hoang Duong and Tsuyoshi Takagi Lattice-Based Dual Receiver Encryption and More Daode Zhang, Kai Zhang, Bao Li, Xianhui Lu, Haiyang Xue and Jie Li Post-Quantum Secure Confidential Transactions (Lattice RingCT v1.0) Wilson Alberto Torres, Ron Steinfeld, Amin Sakzad, Joseph Liu, Nandita Bhattacharjee, Man Ho Au and Jacob Cheng	Session 2B: Symmetric key Cryptography (I) Chair (TBA) Differential Attacks on Reduced Round LILLIPUT Nicolas Marriere, Valerie Nachev and Emmanuel Volte Bounds on the Differential and Linear Branch Number of Permutations Sumanta Sarkar and Habeeb Syed Keyed Sponge with Prefix-Free Padding: Independence between Capacity and Online Queries without the Suffix Key Yusuke Naito
15:50 - 16:10	Coffee Break	
16:10 – 17:25 Session 3A: Room 20-3	Session 3A: Public key Cryptography (I) Chair (TBA) Forward Secure Linkable Ring Signatures Thomas Haines and Xavier Boyen Private Functional Signatures: Definition and Construction Shimin Li, Bei Liang and Rui Xue Linkable Group Signature for Auditing Anonymous Communication Haibin Zheng, Qianhong Wu, Bo Qin, Lin Zhong, Shuangyu He and Jianwei Liu	Session 3B: System and Network Security Chair (TBA) Automatically Identifying Security Bug Reports via Multitype Features Analysis Deqing Zou, Zhijun Deng, Zhen Li and Hai Jin A Practical Privacy Preserving Protocol in Database-driven Cognitive Radio Networks Yali Zeng, Li Xu, Xu Yang and Qikui Xu TDDAD: Time-based Detection and Defense Scheme Against DDoS Attack on SDN Controller Jie Cui, Jiantao He, Yan Xu and Hong Zhong
17:25 – 17:55 Room 20-3	Steering Committee Meeting	
18:00 - 20:00	Welcome Reception	

2018-07-12 (Thursday)

08:30 – 17:25	Registration	
09:30 – 10:30 Room 20-3	<p>Keynote (Chair: Guomin Yang)</p> <p><i>Cognitive biometrics: a new frontier in identity science</i></p> <p><i>Prof. Patrizio Campisi</i></p>	
10:30 – 10:50	Coffee Break	
10:50 – 12:30 Session 4A: Room 20-3	<p>Session 4A: Post-quantum Crypto (II)</p> <p>Chair (TBA)</p> <p>Lattice-Based Universal Accumulator with Efficient Zero-Knowledge Arguments</p> <p>Zuoxia Yu, Man Ho Au, Rupeng Yang, Junzuo Lai and Qiuliang Xu</p> <p>Anonymous Identity-Based Hash Proof System from Lattices in the Standard Model</p> <p>Qiqi Lai, Bo Yang, Yong Yu, Chen Yuan and Liju Dong</p> <p>Complete Attack on RLWE Key Exchange with reused keys, without Signal Leakage</p> <p>Jintai Ding, Scott Fluhrer and Saraswathy Rv</p> <p>Cryptanalysis of the Randomized Version of a Lattice-Based Signature Scheme from PKC'08</p> <p>Haoyu Li, Renzhang Liu, Abderrahmane Nitaj and Yanbin Pan</p>	<p>Session 4B: Foundation (I)</p> <p>Chair (TBA)</p> <p>A Deterministic Algorithm for Computing Divisors in an Interval</p> <p>Liqiang Peng, Yao Lu, Noboru Kunihiro, Rui Zhang and Lei Hu</p> <p>Efficient Bit-Decomposition and Modulus-Conversion Protocols with an Honest Majority</p> <p>Ryo Kikuchi, Dai Ikarashi, Takahiro Matsuda, Koki Hamada and Koji Chida</p> <p>Reusable Fuzzy Extractor from LWE</p> <p>Yunhua Wen and Shengli Liu</p> <p>A Reusable Fuzzy Extractor with Practical Storage Size: Modifying Canetti et.al.'s Construction</p> <p>Jung Hee Cheon, Jinhyuck Jeong, Dongwoo Kim and Jong Chan Lee</p>
12:30 – 13:30	Lunch	
13:30 – 14:30 Room 20-3	<p>Keynote (Chair: Josef Pieprzyk)</p> <p><i>Security and Privacy Challenges in Edge Computing</i></p> <p><i>Dr. Surya Nepal</i></p>	
14:35 – 15:50 Session 5A: Room 20-3	<p>Session 5A: Cloud Security</p> <p>Chair (TBA)</p> <p>Secure Publicly Verifiable Computation with Polynomial Commitment in Cloud Computing</p> <p>Jian Shen, Dengzhi Liu, Xiaofeng Chen, Xinyi Huang, Jiageng Chen and Mingwu Zhang</p> <p>Intrusion-Resilient Public Auditing Protocol for Data Storage in Cloud Computing</p> <p>Yan Xu, Ran Ding, Jie Cui and Hong Zhong</p> <p>Privacy-Preserving Mining of Association Rule on Outsourced Cloud Data from Multiple Parties</p> <p>Lin Liu, Jinshu Su, Rongmao Chen, Ximeng Liu, Xiaofeng Wang, Shu Hofung Leung</p>	<p>Session 5B: Symmetric key Cryptography (II)</p> <p>Chair (TBA)</p> <p>Distributed Time-Memory Tradeoff Attacks on Ciphers (with Application to Stream Ciphers and Counter Mode)</p> <p>Howard Heys</p> <p>New Iterated RC4 Key Correlations</p> <p>Ryoma Ito and Atsuko Miyaji</p> <p>A New Framework for Finding Nonlinear Superpolies in Cube Attacks against Trivium-Like Ciphers</p> <p>Ye Chen-Dong and Tian Tian</p>
15:50 – 16:10	Coffee Break	
16:10 – 17:25 Session 6A: Room 20-3	<p>Session 6A: Public key Cryptography (II)</p> <p>Chair (TBA)</p> <p>Revocable Identity-Based Encryption from the Computational Diffie-Hellman Problem</p> <p>Ziyuan Hu, Shengli Liu, Kefei Chen and Joseph K. Liu</p> <p>Auditable Hierarchy-private Public-key Encryption</p> <p>Lin Zhong, Qianhong Wu, Bo Qin, Haibin Zheng and Jianwei Liu</p> <p>Anonymous Identity-Based Encryption with Identity Recovery</p> <p>Xuecheng Ma, Xin Wang and Dongdai Lin</p>	<p>Session 6B: Short paper (I)</p> <p>Chair (TBA)</p> <p>Enhancing Intelligent Alarm Reduction for Distributed Intrusion Detection Systems via Edge Computing</p> <p>Weizhi Meng, Yu Wang, Wenjuan Li, Zhe Liu, Jin Li and Christian W. Probst</p> <p>ANTSdroid: Automatic Malware Family Behaviour Generation and Analysis for Android Apps</p> <p>Yeali Sun, Shun-Wen Hsiao and Meng Chang Chen</p> <p>Live Path CFI Against Control Flow Hijacking Attacks</p> <p>Mohamad Barbar, Yulei Sui, Hongyu Zhang, Shiping Chen and Jingling Xue</p> <p>Improving the BKZ Reduction Algorithm by Quick Reordering Technique</p> <p>Yuntao Wang and Tsuyoshi Takagi</p> <p>CRT-KPS: A Key Predistribution Schemes Using CRT</p> <p>Pinaki Sarkar, Mayank Baranwal and Sukumar Nandi</p>
18:30 - 22:00	<p>Conference Banquet</p> <p>Harbourfront Seafood Restaurant, 2 Endeavour Dr, Wollongong</p>	

2018-07-13 (Friday)

08:30 – 12:30	Registration	
09:30 - 10:20 Session 7A: Room 20-3	Session 7A: Security Protocol Chair (TBA) Secure Contactless Payment Handan Kilinc and Serge Vaudenay	Session 7B: Public key Cryptography (III) Chair (TBA) Key-updatable Public-key Encryption with Keyword Search: Models and Generic Constructions Hiroaki Anada, Akira Kanaoka, Natsume Matsuzaki and Yohei Watanabe
Session 7B: Room 20-2	New Attacks and Secure Design for Anonymous Distance-Bounding Ahmad Ahmadi, Reihaneh Safavi-Naini and Mamunur Akand	Asymmetric Subversion Attacks on Signature Schemes Chi Liu, Rongmao Chen, Yi Wang and Yongjun Wang
10:20 – 10:50	Coffee Break	
10:50 – 12:30 Session 8A: Room 20-3	Session 8A: Foundation (II) Chair (TBA) 21 - Bringing Down the Complexity: Fast Composable Protocols for Card Games Without Secret State Bernardo David, Rafael Dowsley and Mario Larangeira	Session 8B: Short paper (II) Chair (TBA) Practical Signatures from the Partial Fourier Recovery Problem Revisited: A Provably-Secure and Gaussian-Distributed Construction Xingye Lu, Zhenfei Zhang and Man Ho Au
Session 8B: Room 20-2	Verifiable secret sharing based on hyperplane geometry with its applications to optimal resilient proactive cryptosystems Zhe Xia, Liuying Sun, Bo Yang, Yanwei Zhou and Mingwu Zhang Towards Round-Optimal Secure Multiparty Computations: Multikey FHE without a CRS Eunhyung Kim, Hyang-Sook Lee and Jeongeun Park Robust Multiparty Computation with Faster Verification Time Souradyuti Paul and Ananya Shrivastava	Revocable Certificateless Encryption with Ciphertext Evolution Yinxia Sun, Futai Zhang and Anmin Fu A New Encryption Scheme Based on Rank Metric Codes Terry S. C. Lau and Chik How Tan Security Analysis and Modification of ID-Based Encryption with Equality Test from ACISP 2017 Hyung Tae Lee, Huaxiong Wang and Kai Zhang Constant-Size CCA-Secure Multi-hop Unidirectional Proxy Re-Encryption from Indistinguishability Obfuscation Junzuo Lai, Zhengang Huang, Man Ho Au and Xianping Mao
12:30 – 12:40 Room 20-3	Conference Closing	
12:40– 13:40	Lunch	