ACISP 2013 Program

Australasian Conference on Information Security and Privacy

Queensland University of Technology, Gardens Point, Brisbane

www.acisp2013.qut.edu.au

Monday 1 July

8:15 – 9:00	DELEGATE REGISTRATION: On arrival, please proceed to the registration desk outside the Kindler Theatre (room P421). *All sessions take place in the Kindler Theatre.*
9.00 – 10.30	Session 1
9.00 – 9.30	Welcome
9.30 – 10.30	**Keynote speaker**: *Paul Ashley*, IBM Security Systems Trends in Advanced Threat Protection
10.30 – 11.00	Morning tea
11.00 – 12.15	Session 2: Cryptanalysis I
	Chris Mitchell – Analysing the IOBC Authenticated Encryption Mode
	Subhadeep Banik, Subhamoy Maitra, Santanu Sarkar, Meltem Sonmez Turan – A Chosen IV Related Key Attack on Grain-128a
	Zhenqing Shi, Bin Zhang, Dengguo Feng – Cryptanalysis of Helix and Phelix Revisited
12.15 – 13.15	Lunch | OJW Room, level 12, S block
13.15 – 14.55	Session 3: RSA | the Kindler Theatre
	Hui Zhang, Tsuyoshi Takagi – Attacks on Multi-Prime RSA with Small Prime Difference
	Yao Lu, Rui Zhang, Dongdai Lin – Factoring Multi-Power RSA Modulus with Partial Known Bits
	Masayuki Fukumitsu, Shingo Hasegawa, Shuji Isobe, Eisuke Koizumi, Hiroki Shizuya – Toward Separating the Strong Adaptive Pseudo-Freeness from the Strong RSA Assumption
	Yoshinori Aono – Minkowski Sum Based Lattice Construction for Multivariate Simultaneous Coppersmith's Technique and Applications to RSA
14.55 – 15.20	Afternoon tea
15.20 – 17.00	Session 4: Lattices and Security Proofs
	Thomas Plantard, Willy Susilo, Zhenfei Zhang – Adaptive Precision Floating Point
	Atsushi Takayasu, Noboru Kunihiro – Better Lattice Constructions for Solving Multivariate Linear Equations Modulo Unknown Divisors
	Baodong Qin, Shengli Liu, Zhengan Huang – Key-Dependent Message Chosen-Ciphertext Security of the Cramer-Shoup Cryptosystem
	Ahto Buldas, Margus Niitsoo – Black-Box Separations and their Adaptability to the Non-Uniform Model

Tuesday 2 July

9.00 – 10.40	Session 1: Public Key Cryptography
	Hiroaki Anada, Seiko Arita, Sari Handa, Yosuke Iwabuchi – Attribute-Based Identification: Definitions and Efficient Constructions
	Yang Wang, Mark Manulis, Man Ho Au, Willy Susilo – Relations among Privacy Notions for Signcryption and Key Invisible "Sign-then-Encrypt"
	Pierre-Alain Fouque, Antoine Joux, Mehdi Tibouchi – Injective Encodings to Elliptic Curves
	Fuchun Guo, Yi Mu, Willy Susilo, Vijay Varadharajan – Membership Encryption and its Applications

10.40 – 11.00	Morning tea
11.10 – 12.00	Session 2: Hashing
	Ahto Buldas, Risto Laanoja: Security Proofs for Hash Tree Time-Stamping using Hash Functions with Small Output Size
	Dongxia Bai, Hongbo Yu, Gaoli Wang, Xiaoyun Wang: Improved Boomerang Attacks on SM3
12.00 – 13.00	**Keynote speaker**: *Xavier Boyen*, Queensland University of Technology Excessive Cryptography: Lattice Perspectives
13.00 – 14.00	Lunch | OJW Room, level 12, S block
14.00 – 15.15	Session 3: Cryptanalysis II
	Takanori Isobe, Yu Sasaki, Jiageng Chen – Related-Key Boomerang Attacks on KATAN32/48/64
	Junko Takahashi, Toshinori Fukunaga, Kazumaro Aoki, Hitoshi Fuji – Highly Accurate Key Extraction Method for Access-Driven Cache Attacks Using Correlation Coefficient
	Yosuke Todo – Upper Bounds for the Security of Several Feistel Networks
15.15 – 15.40	Afternoon tea
15.40 – 16.30	Session 4: Signatures
	Willy Susilo, Man Ho Au, Yang Wang, Duncan Wong – Fairness in Concurrent Signatures Revisited
	Essam Ghadafi – Formalizing Group Blind Signatures and Practical Constructions without Random Oracles
16.30 – 17.30	**Keynote speaker:** *Bradley Schatz,* Schatz Forensic Current and future challenges in digital forensics
18:30 – 22:00	Conference dinner

Wednesday 3 July

9.00 – 10.40	Session 1: Passwords and mobile security
	Byoung-Il Kim, Jin Hong – Analysis of the Non-Perfect Table Fuzzy Rainbow Tradeoff
	Seyit Camtepe – Complexity of Increasing the Secure Connectivity in Wireless Ad Hoc Networks
	George Petrides, Kristian Gjøsteen, Asgeir Steine – Towards Privacy Preserving Mobile Internet Communications: How Close Can We Get?
	Leah South, Douglas Stebila – Count-Min Sketches for Estimating Password Frequency with Hamming Distance at Most Two
10.40 – 11.10	Morning tea
11.10 – 12.00	Session 2: Secret sharing
	Yang Yu, Zhanfei Zhou – A Rational Secret Sharing Protocol with Unconditional Security in the Synchronous Setting
	Ryo Kikuchi, Koji Chida, Dai Ikarashi, Koki Hamada, Katsumi Takahashi – Secret Sharing Schemes with Conversion Protocol to Achieve Short Share-Size and Extendibility to Multiparty Computation
12.00 – 13.00	**Keynote speaker:** *Yuliang Zheng*, University of North Carolina Public Key Cryptography for Mobile Cloud
13:00 – 14:00	Lunch | OJW Room, level 12, S block