QUT ife
Institute for Future Environments

Australasian Conference on Information Security and Privacy 2015 Program

Queensland University of Technology, Gardens Point, Brisbane | www.acisp2015.qut.edu.au

Monday, 29 June 2015

8:30 – 9:15am	**DELEGATE REGISTRATION**
9.15 – 10.30am	**SESSION 1: Welcome and keynote**
9.15 – 9.30am	Welcome and opening address
9.30 – 10.30am	**Keynote**: *How cryptography politics influences cryptography research* Colin Boyd, Norwegian University of Science and Technology
10.30 – 11.00am	Morning tea
11.00 – 12.15am	**SESSION 2: Symmetric cryptanalysis 1**
	Weak-key and Related-key Analysis of Hash-Counter-Hash Tweakable Enciphering Schemes -Zhelei Sun, Peng Wang and Liting Zhang
	Cryptanalysis of Whirlwind - Bingke Ma, Bao Li, Ronglin Hao and Xiaoqian Li
	Improving the Biclique Cryptanalysis of AES – Biaoshuai Tao and Hongjun Wu
12:15 – 12:20pm	Group photo
12.20 – 1.15pm	Lunch
1.15 – 2.55pm	**SESSION 3: Public key cryptography**
	A New General Framework for Secure Public Key Encryption with Keyword Search - Rongmao Chen, Yi Mu, Guomin Yang, Fuchun Guo and Xiaofen Wang
	Dynamic Threshold Public-key Encryption with Decryption Consistency from Static Assumptions - Yusuke Sakai, Keita Emura, Jacob C.N. Schuldt, Goichiro Hanaoka and Kazuo Ohta
	Sponge based CCA2 secure asymmetric encryption for arbitrary length message - Tarun Kumar Bansal, Donghoon Chang and Somitra Kumar Sanadhya
	Trade-off Approaches for Leak Resistant Modular Arithmetic in RNS - Christophe Negre and Guilherme Perin
2.55 – 3.25pm	Afternoon tea
3.25 – 5.05pm	**SESSION 4: Identity-based encryption**
	Towards Forward Security Properties for PEKS and IBE - Qiang Tang
	IBE under k-LIN with Shorter Ciphertexts and Private Keys - Kaoru Kurosawa and Le Trieu Phong
	Improved Identity-Based Online/Offline Encryption - Jianchang Lai, Yi Mu and Fuchun Guo
	Constructions of CCA-secure Revocable Identity-based Encryption - Yuu Ishida, Yohei Watanabe and Junji Shikata

Tuesday, 30 June 2015

9.30 – 10.45am	**SESSION 1: Digital signatures**
	Linkable Message Tagging: Solving the key distribution problem of signature schemes - Felix Günther and Bertram Poettering
	Generic Transformation to Strongly Existentially Unforgeable Signature Schemes with Continuous Leakage Resiliency - Yuyu Wang and Keisuke Tanaka
	Constant Size Ring Signature Without Random Oracle - Priyanka Bose, Dipanjan Das and Pandu Rangan Chandrasekharan
10.45 – 11.15am	Morning tea

11.15 – 12.15pm	**SESSION 2: Keynote**
	Keynote: *Security in the wild - challenges and opportunities of helping to protect millions of customers* Simon Pope, Microsoft Security Response Center
12.15 – 1.15pm	Lunch
1.15 – 2.55pm	**SESSION 3: Security and protocols**
	Constant-Round Leakage-Resilient Zero-Knowledge Argument for NP from the Knowledge-of-Exponent Assumption - Tingting Zhang, Hongda Li and Guifang Huang
	Modelling ciphersuite and version negotiation in the TLS protocol - Benjamin Dowling and Douglas Stebila
	VisRAID: Visualizing Remote Access for Intrusion Detection - Laleil Trehothan, Craig Anslow, Stuart Marshall and Ian Welch
	BP-XACML: an authorisation policy language for business process - Khalid Alissa, Ed Dawson, Farzad Salim and Jason Reid
2.55 – 3.25pm	Afternoon tea
3.25 – 4.40pm	**SESSION 4: Symmetric cryptanalysis 2**
	How TKIP induces biases of internal states of generic RC4 - Ryoma Ito and Atsuko Miyaji
	Preventing Fault Attack using Fault Randomization with a case study on AES – Shamit Ghosh, Dhiman Saha, Abhrajit Sengupta and Dipanwita Roy Chowdhury
	Analysis of Rainbow Tables with Fingerprints - Gildas Avoine, Adrien Bourgeois and Xavier Carpent
6:30 – 9:30pm	**Conference dinner** | Port Office Hotel

Wednesday, 1 July 2015

9.30 – 10.45am	**SESSION 1: Privacy protocols**
	A New Public Remote Integrity Checking Scheme with User Privacy - Yiteng Feng, Yi Mu and Guomin Yang
	Efficient Dynamic Provable Data Possession with Public Verifiability and Data Privacy - Clémentine Gritti, Willy Susilo and Thomas Plantard
	Privately Computing Set-Union and Set-Intersection Cardinality via Bloom Filters - Rolf Egert, Marc Fischlin, David Gens, Sven Jacob, Matthias Senker and Jörn Tillmanns
10.45 – 11.15am	Morning tea
11.15 – 12.15pm	**SESSION 2: Keynote**
	Keynote: *Partnership for cyber resilience* Jason Smith, CertAust
12.15 – 1.15pm	Lunch
1.15 – 2.05pm	**SESSION 3: Symmetric constructions**
	Generalizing PMAC under Weaker Assumptions - Nilanjan Datta and Kan Yasuda
	sp-AELM: Sponge based Authenticated Encryption Scheme for Memory Constrained Devices - Megha Agrawal, Donghoon Chang and Somitra Sanadhya
2.05 – 2.35pm	Afternoon tea
2.35 – 3.25pm	**SESSION 4: Homomorphic encryption and obfuscation**
	Secure statistical analysis by LWE-based homomorphic encryption - Masaya Yasuda, Takeshi Shimoyama, Jun Kogure, Kazuhiro Yokoyama and Takeshi Koshiba
	Bad directions in cryptographic hash functions - Daniel J. Bernstein, Andreas Hülsing, Tanja Lange and Ruben Niederhagen
3.25 – 3.30pm	Closing address
4.00 – 5.30pm	**HYPOTHETICAL EVENT** | Kindler Theatre, Science & Engineering Centre (GP-P421) Expert panellists discuss: *Cyber-attack hits Brisbane: how prepared are we?*