ACISP 2021 Program

Time (Sydney)	Dec 1	Dec 2	Dec 3
10:00-10:15	**Inauguration**	**Jennifer Seberry Lecture** Presenter: **Josef Pieprzyk** Session Chair: Jennifer Seberry	**Keynote Talk** Presenter: **David Liebowitz** Session Chair: Surya Nepal
10:15-11:00	**Keynote Talk** Presenter: **Ron Steinfeld** Session Chair: Joonsang Baek		
11:15-11:30 (Dec 1) 11:00-11:30 (Dec 2, Dec 3)	Break	Break	Break
11:30-12:30	**Session 1:** Cryptographic Foundations	**Session 4:** Privacy	**Session 7:** Blockchain – Analysis and Attack
12:30-13:30	Lunch	Lunch	Lunch
13:30-14:30	**Session 2:** Encryption	**Session 5:** Blockchain – Protocols and Foundations	**Session 8:** Symmetric Primitive & Post Quantum Cryptography I
14:30- 15:30	**Session 3:** Post Quantum Cryptography - Encryption	**Session 6:** Privacy for Machine Learning	**Session 9:** Symmetric Primitive & Post Quantum Cryptography II
15:30- 16:00	Break	Break	Break
16:00- 17:00	**Rump Session**	**Keynote Talk** Presenter: **Nishanth Chandran** Session Chair: Khoa Nguyen	**Steering Committee Meeting**
17:00- 18:00	Dinner	Australasia Researcher's meet & Dinner	
18:00- 19:00	**Keynote Talk** Presenter: **Pierangela Samarati** Session Chair: Sushmita Ruj	**Australasia Researchers' meet** Best paper ACISP 2022 announcement & Dinner	
19:00-20:00		**Keynote Talk** Presenter: **Aggelos Kiayias** Session Chair: Joseph Liu	

Session 1: Cryptographic Foundations

Session Chair: Shashank Agrawal, Western Digital Research

Leakage Resilient Cheating Detectable Secret Sharing Schemes - Sabyasachi Dutta and Reihaneh Safavi-Naini

Chosen Ciphertext Secure Functional Encryption from Constrained Witness PRF - Tapas Pal and Ratna Dutta

Updatable Trapdoor SPHFs: Modular Construction of Updatable Zero-Knowledge Arguments and More - Behzad Abdolmaleki and Daniel Slamanig

Small Superset and Big Subset Obfuscation - Steven D. Galbraith and Trey Li

Session 2: Encryption

Session Chair: Fuchun Guo, University of Wollongong

Broadcast Authenticated Encryption with Keyword Search - Xueqiao Liu, Kai He, Guomin Yang, Willy Susilo, Joseph Tonien, and Qiong Huang

An Anonymous Trace-and-Revoke Broadcast Encryption Scheme - Olivier Blazy, Sayantan Mukherjee, Huyen Nguyen, Duong Hieu Phan, and Damien Stehlé 214

Security Analysis of End-to-End Encryption for Zoom Meetings - Takanori Isobe and Ryoma Ito

CCA Secure Attribute-Hiding Inner Product Encryption from Minimal Assumption - Tapas Pal and Ratna Dutta

Session 3: Post Quantum Cryptography - Encryption

Session Chair: Veronika Kucha, University of Queensland

Puncturable Identity-Based Encryption from Lattices - Priyanka Dutta, Willy Susilo, Dung Hoang Duong, and Partha Sarathi Roy

Optimizing Bootstrapping and Evaluating Large FHE Gates in the LWE-Based GSW-FHE - Chao Liu, Anyu Wang, and Zhongxiang Zheng

Forward-Secure Group Encryptions from Lattices - Jing Pan, Xiaofeng Chen, Fangguo Zhang, and Willy Susilo

Anonymous Lattice Identity-Based Encryption with Traceable Identities - Xavier Boyen, Ernest Foo, and Qinyi Li

Session 4: Privacy

Session Chair: Hyoungshick Kim, Sungkyunkwan University

Optimal Randomized Partial Checking for Decryption Mix Nets - Thomas Haines and Johannes Müller

A Novel Proof of Shuffle: Exponentially Secure Cut-and-Choose - Thomas Haines and Johannes Müller

Private Decision Tree Evaluation with Constant Rounds via (Only)Fair SS-4PC - Hikaru Tsuchida and Takashi Nishide

Partially-Fair Computation from Timed-Release Encryption and Oblivious Transfer - Geoffroy Couteau, A. W. Roscoe, and Peter Y. A. Ryan

Session 5: Blockchain - Protocols and Foundations

Session Chair: Allen Man Ho Au, University of Hong Kong

A Secure Cross-Shard View-Change Protocol for Sharding Blockchains - Yizhong Liu, Jianwei Liu, Yiming Hei, Yu Xia, and Qianhong Wu

Efficient Unique Ring Signature for Blockchain Privacy Protection - Anh The Ta, Thanh Xuan Khuc, Tuong Ngoc Nguyen, Huy Quoc Le, Dung Hoang Duong, Willy Susilo, Kazuhide Fukushima, and Shinsaku Kiyomoto

Redactable Transactions in Consortium Blockchain: Controlled by Multi-authority CP-ABE - Zongyang Zhang, Tong Li, Zhuo Wang, and Jianwei Liu

Concise Mercurial Subvector Commitments: Definitions and Constructions - Yannan Li, Willy Susilo, Guomin Yang, Tran Viet Xuan Phuong, Yong Yu, and Dongxi Liu

Session 6: Privacy for Machine Learning

Session Chair: Dan Kim, University of Queensland

ALRS: An Adversarial Noise Based Privacy-Preserving Data Sharing Mechanism - Jikun Chen, Ruoyu Deng, Hongbin Chen, Na Ruan, Yao Liu, Chao Liu, and Chunhua Su

Non-interactive, Secure Verifiable Aggregation for Decentralized, Privacy-Preserving Learning - Carlo Brunetta, Georgia Tsaloli, Bei Liang, Gustavo Banegas, and Aikaterini Mitrokotsa

Machine Learning - Analysis and Attack Towards Visualizing and Detecting Audio Adversarial Examples for Automatic Speech Recognition - Wei Zong, Yang-Wai Chow, and Willy Susilo

Oriole: Thwarting Privacy Against Trustworthy Deep Learning Models - Liuqiao Chen, Hu Wang, Benjamin Zi Hao Zhao, Minhui Xue, and Haifeng Qian

Session 7: Blockchain - Analysis and Attack

Session Chair: Guomin Yang, University of Wollongong

Transparency or Anonymity Leak: Monero Mining Pools Data Publication - Dimaz Ankaa Wijaya, Joseph K. Liu, Ron Steinfeld, and Dongxi Liu

Mind the Scraps: Attacking Blockchain Based on Selfdestruct - Wei-Yang Chiu and Weizhi Meng

A Blockchain-Enabled Federated Learning Model for Privacy Preservation: System Design - Minfeng Qi, Ziyuan Wang, Fan Wu, Rob Hanson, Shiping Chen, Yang Xiang, and Liming Zhu

Session 8: Symmetric Primitive & Post Quantum Cryptography I

Session Chair: Dongxi Liu, Data61 CSIRO
Algebraic Attacks on Round-Reduced Keccak - Fukang Liu, Takanori Isobe, Willi Meier, and Zhonghao Yang

On MILP-Based Automatic Search for Bit-Based Division Property for Ciphers with (Large) Linear Layers - Muhammad ElSheikh and Amr M. Youssef

Authentication Lattice-Based Secure Biometric Authentication for Hamming Distance - Jung Hee Cheon, Dongwoo Kim, Duhyeong Kim, Joohee Lee, Junbum Shin, and Yongsoo Song

A Trustless GQ Multi-signature Scheme with Identifiable Abort - Handong Cui and Tsz Hon Yuen

Session 9: Symmetric Primitives & Post Quantum Cryptography II

Session Chair: Clementi Gritti, University of Canterbury

Constructions of Iterative Near-MDS Matrices with the Lowest XOR Count - Xiaodan Li and Wenling Wu

Forced Independent Optimized Implementation of 4-Bit S-Box - Yanhong Fan, Weijia Wang, Zhihu Li, Zhenyu Lu, Siu-Ming Yiu, and Meiqin Wang

Distinguishing and Key Recovery Attacks on the Reduced-Round SNOW-V - Jin Hoki, Takanori Isobe, Ryoma Ito, Fukang Liu, and Kosei Sakamoto

Verifiable Obtained Random Subsets for Improving SPHINCS+ - Mahmoud Yehia, Riham AlTawy, and T. Aaron Gulliver