## ACISP 2021 Program

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

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

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

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

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

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

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

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

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

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

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