Local Time	Day 1 (14 July)	
08:00-08:30	Registration (Buidling 20.Room 2)	
08:30-09:00	Welcome Coffee	
09:00-09:30	Opening & Photo	
09:30-10:30	Jennifer Seberry Lecture Title: The Evolution of Cybersecurity Research at CSIRO: A Two-Decade Journey and Future Outlook Speaker: Surya Nepal Session Chair: XXX	
10:30-11:00	Coffee Break	
11:00-12:20	Session 1A (4 papers) (Session Chair: XXX)	Session 1B (4 papers) (Session Chair: XXX)
12:30-14:00	Lunch	
14:00-16:00	Session 2A (6 papers) (Session Chair: XXX)	Session 2B (6 papers) (Session Chair: XXX)
16:00-16:30	Coffee Break	
16:30-17:10	Session 3 (2 papers) (Session Chair: XXX)	
17:20-17:50	Special Event: In Memory of Ed Dawson (Session Chair: XXX)	
18:00-19:30	Dinner: Pizza Night Location: XXX	

=================================DAY 1=================================

Session 1A: Cryptographic Foundations and Number Theory

1. Compact Lifting for NTT-unfriendly Modulus (Ying Liu, Xianhui Lu, Yu Zhang, Ruida Wang, Ziyao Liu, Kunpeng Wang)
2. Guaranteed Termination Asynchronous Complete Secret Sharing with Lower Communication and Optimal Resilience (Ying Cai, Chengyi Qin, Mingqiang Wang)
3. Solving Generalized Approximate Divisor Multiples Problems (Naoki Shimoe, Noboru Kunihiro)
4. Improving RSA Cryptanalysis: Combining Continued Fractions and Coppersmith's Techniques (Mengce Zheng, Yansong Feng, Abderrahmane Nitaj, Yanbin Pan)

Session 1B: AI Security and Privacy (1)

1. Identifying the Truth of Global Model: A Generic Solution to Defend Against Byzantine and Backdoor Attacks in Federated Learning (Sheldon C. Ebron, Meiying Zhang, Kan Yang)
2. RAGLeak: Membership Inference Attacks on RAG-based Large Language Models (Kaiyue Feng, Guangsheng Zhang, Huan Tian, Heng Xu, Yanjun Zhang, Tianqing Zhu, Ming Ding, Bo Liu)
3. DeGain: Detecting GAN-based Data Inversion in Collaborative Deep Learning (Zhenzhu Chen, Yansong Gao, Anmin Fu, Fanjian Zeng, Boyu Kuang, Robert H. Deng)
4. FRFL: Fair and Robust Federated Learning Incentive Model Based on Game Theory (Haocheng Ye, Lu Zhou, Hao Wang, Chunpeng Ge)

Session 2A: Digital Signatures and Zero Knowledge

1. Compressed Sigma Protocols: New Model and Aggregation Techniques (Yuxi Xue, Tianyu Zheng, Shang Gao, Bin Xiao, Man Ho Au)
2. Glitter: A Fully Adaptive and Tightly Secure Threshold Signature (Shaolong Tang, Peng Jiang, Liehuang Zhu)
3. Faster VOLEitH Signatures from All-but-One Vector Commitment and Half-Tree (Dung Bui, Kelong Cong, Cyprien Delpech de Saint Guilhem)
4. Efficient Multi-instance Vector Commitment and Application to Post-quantum Signatures (Dung Bui)
5. Three-Round (Robust) Threshold ECDSA from Threshold CL Encryption (Bowen Jiang, Guofeng Tang, Haiyang Xue)
6. Lattice Attack with EHNP: Key Recovery from Two ECDSA Signatures and Breaking the Information-Theoretic Limit (Tianyou Tang, Shuqin Fan)

Session 2B: System and Software Security

1. Bridging Clone Detection and Industrial Compliance: A Practical Pipeline for Enterprise Codebases (Xiaowei Zhang, Shigang Liu, Jun Zhang, Yang Xiang)
2. Mitigating the Unprivileged User Namespaces based Privilege Escalation Attacks with Linux Capabilities (Jingzi Meng, Yuewu Wang, Lingguang Lei, Chunjing Kou, Peng Wang, Huawei Lu)
3. Ransomware Encryption Detection: Adaptive File System Analysis Against Evasive Encryption Tactics (Arash Mahboubi, Hamed Aboutorab, Seyit Camtepe, Hang Thanh Bui, Khanh Luong, Keyvan Ansari, Shenlu Wang, Bazara Barry)
4. SoK: From Systematization to Best Practices in Fuzz Driver Generation (Qian Yan, Minhuan Huang, Huayang Cao, Shuaibing Lu)
5. Facial Authentication Security Evaluation against Deepfake Attacks in Mobile Apps (Chuer Yu, Haoyu Wang, Xia Liu, Zonghui Wang, Lirong Fu, Zhiyuan Wan, Yandong Gao, Yang Xiang, Wenzhi Chen)
6. Shortest Printable Shellcode Encoding Algorithm Based on Dynamic Bitwidth Selection (Guoan Liu, Jian Lin, Weiyu Dong, Jiaan Liu, Tieming Liu)

Session 3:

1. Zeroth-Order Federated Private Tuning for Pretrained Large Language Models (Xiaoyu Zhang, Yong Lin, Meixia Miao, Jian Lou, Jin Li, Xiaofeng Chen)
2. Unbounded Multi-Hop Proxy Re-Encryption with HRA Security: An LWE-Based Optimization (Xiaohan Wan, Yang Wang, Haiyang Xue, Mingqiang Wang)

Local Time	Day 2 (15 July)	
08:45-09:00	Registration	
09:00-10:00	Keynote Session Title: KEMs and Their Applications to Quantum-Safe Communications Speaker: Rei Safavi-Naini, Session Chair: XXX	
10:00-10:30	Coffee Break	
10:30-11: 50	Session 4A (4papers) (Session Chair: XXX)	Session 4B (4 papers) (Session Chair: XXX)
12:00-12:30	Special Event: 30th ACISP Memory (Session Chair: XXX)	
12:30-14:00	Lunch	
14:00-16:00	Session 5A (4 papers) (Session Chair: XXX)	Session 5B (6 papers) (Session Chair: XXX)
16:00-16:20	Coffee Break	
16:20-17:20	ACISP Steering Committee Meeting (Room 2)	
17:20-18:00	Travel to Banquet (Free Bus 55A)	
18:00-22:00	Banquet Location: Harbourfront Seafood Restaurant Address: 2 Endeavour Dr, Wollongong Note: Use your name badge to check in	

=================================DAY 2=================================

Session 4A: Post-Quantum Cryptography (1)

1. Partial Key Exposure Attacks on UOV and Its Variants (Yuki Seto, Hiroki Furue, Atsushi Takayasu)
2. Fiat-Shamir with Rejection and Rotation (Xianhui Lu, Yongjian Yin, Dingding Jia, Jingnan He, Yamin Liu, Yijian Liu, Hongbo Liu)
3. Amoeba: More Flexible RLWE-based KEM (Qingfeng Wang, Li-Ping Wang)
4. Get Rid of Templates: A Chosen-Ciphertext Attack on ML-KEM with a DPA-based Self-Comparison Oracle (Zhenzhi Lai, Udaya Parampalli)

Session 4B: Privacy Enhancing Technologies (1)

1. Comparing and Improving Frequency Estimation Perturbation Mechanisms under Local Differential Privacy (She Sun, Jiafei Wu, Jian Yang, Li Zhou, Huiwen Wu)
2. Strong Federated Authentication with Password-based Credential against Identity Server Corruption (Changsong Jiang, Chunxiang Xu, Guomin Yang, Li Duan, Jing Wang)
3. Anonymous Credentials with Credential Redaction and Its Application to SSI-based Plug&Charge for Shared Vehicles (Kyosuke Hatsugai, Kyoichi Asano, Yuki Sawai, Yohei Watanabe, Mitsugu Iwamoto)
4. EAPIR: Efficient and Authenticated Private Information Retrieval With Fast Server Processing (Hua Shen, Xinjie Li, Zhen Fan, Ge Wu, Mingwu Zhang)

Session 5A: Privacy Enhancing Technologies (2)

1. Direction-Oriented Smooth Sensitivity and Its Application to Genomic Statistical Analysis (Akito Yamamoto, Tetsuo Shibuya)
2. Sentence Embedding Generation Method for Differential Privacy Protection (Yangyang Liu, Wanqi Wang, Jingyu Hua)
3. KD-IBMRKE-PPFL: A Privacy-Preserving Federated Learning Framework Integrating Knowledge Distillation and Identity-Based Multi-Receiver Key Encapsulation (Yuan Li, Changji Wang, Shiwen Hu)
4. Robust and Privacy-Preserving Dynamic Average Consensus with Individual Weight (Yuanyuan Zhang, Yu Liu, Yahui Wang, Tianqing Zhu, Mingwu Zhang)

Session 5B: Encryption and Homomorphic

1. Ideal Transformations for Public Key Encryption (Yao Cheng, Xianhui Lu, Ziyi Li)
2. Receiver-initiated Updatable Public Key Encryption: Construction, Security and Application (Jiahao Xuan)
3. Indifferentiability Separations in Ideal Public Key Encryption: Explicit vs. Implicit Rejection (Yao Cheng, Xianhui Lu, Ziyi Li, Yongjian Yin)
4. Accountability for Server Misbehavior in Homomorphic Secret Sharing (Xinzhou Wang, Shi-Feng Sun, Dawu Gu, Yuan Luo)
5. High-Precision Homomorphic Modular Reduction for CKKS Bootstrapping (Zejiu Tan, Junping Wan, Zoe L. Jiang, Jingjing Fan, Manho Au, Siuming Yiu)
6. Refined Error Management for Gate Bootstrapping (Chunling Chen, Xianhui Lu, Binwu Xiang, Bowen Huang, Ruida Wang, Yijian Liu)

Local Time	Day 3 (16 July)	
08:45-09:00	Registration	
09:00-10:00	Keynote Session Title: A Multi-Enclave Architecture for Blockchains Admitting Proof of Useful Work for Consensus Speaker: Yuliang Zheng, Session Chair: XXX	
10:00-10:30	Coffee Break	
10:30-12: 30	Session 6A (6 papers) (Session Chair: XXX)	Session 6B (6 papers) (Session Chair: XXX)
12:30-14:00	Lunch	
14:00-15:40	Session 7A (5papers) (Session Chair: XXX)	Session 7B (4papers) (Session Chair: XXX)
15:40-16:00	Closing	

=================================DAY 3================================

Session 6A: Cryptographic Protocols and Blockchain

1. FlexiADKG: A Flexible Asynchronous Distributed Key Generation Protocol with Constant Round Complexity (Yang Yang, Bingyu Li, Zhenyang Ding, Qianhong Wu, Bo Qin, Qin Wang)
2. TEAKEX: TESLA-Authenticated Group Key Exchange (Qinyi Li, Lise Millerjord, Colin Boyd)
3. SoK: A Deep Dive into Anti-Money Laundering Techniques for Blockchain Cryptocurrencies (Qishu Huang Fu, Joseph K. Liu, Shirui Pan, Tsz Hon Yuen)
4. Advanced Temporal Graph Embedding For Detecting Fraudulent Transactions on Complex Blockchain Transactional Networks (Jianbin Gao, Ansu Badjie, Qi Xia, Patrick Mukala, Hu Xia, Grace Mupoyi Ntuala)
5. Walnut: A Generic Framework with Enhanced Scalability for BFT Protocols (Lei Tian, Chenke Wang, Yu Long, Xian Xu, Mingchao Wan, Chunmiao Li, Shi-Feng Sun, Dawu Gu)
6. PPSCCC: Privacy-Preserving Scalable Cross-Chain Communication Among Multiple Blockchains Based on Parent-Child Blockchain (Hideaki Miyaji, Noriaki Kamiyama)

Session 6B: Symmetric-Key Cryptography and Cryptanalysis

1. Forgery Attacks on SipHash (Kosuke Sasaki, Rikuto Kurahara, Kosei Sakamoto, Takanori Isobe)
2. Cryptanalysis of Fruit-F: Exploiting Key-Derivation Weaknesses and Initialization Vulnerabilities (Subhadeep Banik, Hailun Yan)
3. Exploring Key-Recovery-Friendly Differential Distinguishers for SM4 and Their Performance in Differential Attacks (Bingqing Li, Ling Sun)
4. Inner Product Masked Integral Distinguishers and Integral Sets over Large Finite Fields Applications to MiMC, CIMINION and Chaghri (Weizhe Wang, Deng Tang, Haoyang Wang)
5. Improved Differential Meet-In-The-Middle Cryptanalysis on SIMON and Piccolo (Weiqing Deng, Jianing Zhang, Haoyang Wang)
6. Strengthening Key Scheduling of AES-256 with Minimal Software Modifications (Shoma Kawakami, Kazuma Taka, Atsushi Tanaka, Tatsuya Ishikawa, Takanori Isobe)

Session 7A: AI Security and Privacy (2)

1. MG-Det: Deepfake Detection with Multi-Granularity (Ahmed Asiri, Luoyu Chen, Zhiyi Tian, Xiaoyu Ding, Shui Yu)
2. LPIA: Label Preference Inference Attack against Federated Graph Learning (Jiaxue Bai, Lu Shi, Yang Liu, Weizhe Zhang)
3. DPFedSub: A Differentially Private Federated Learning with Randomized Subspace Descend (Huiwen Wu, Chuan Ma, Xueran Li, Deyi Zhang, Xiaohan Li, She Sun) ZOOM
4. DARA: Enhancing Vulnerability Alignment via Adaptive Reconstruction and Dual-Level Attention (Lihua Wang, Jiaojiao Jiang, Salil S. Kanhere, Jiamou Sun, Sanjay Jha, Zhenchang Xing)
5. Understanding the Robustness of Machine Unlearning Models (Guanqin Zhang, Feng Xu, H.M.N. Dilum Bandara, Shiping Chen, Yulei Sui)

Session 7B: Post-Quantum Cryptography (2)

1. Towards Quantum Security of Hirose Compression Function and Romulus-H (Shaoxuan Zhang, Chun Guo, Meiqin Wang)
2. Breaking the Shield: Novel Fault Attacks on CRYSTALS-Dilithium (Dixiao Du, Yuejun Liu, Yiwen Gao, Jingdian Ming, Hao Yuan, Yongbin Zhou)
3. Efficient Revocable Identity-Based Encryption from Middle-Product LWE (Takumi Nishimura, Atsushi Takayasu)
4. Code-based Fully Dynamic Accountable Ring Signatures and Group Signatures using the Helper Methodology (Rishiraj Bhattacharyya, Sreehari Kollath, Christophe Petit)