ICISC 2020 Program

Wednesday, (2020-12-02)	
KST 09:20 – 09:30 UTC 00:20 – 00:30	**Opening Remarks**
KST 09:30 – 10:20 UTC 00:30 – 01:20	**Session 1: Security Models** Security Definitions on Time-Lock Puzzles Daiki Hiraga, Keisuke Hara, Masayuki Tezuka Yusuke Yoshida, Keisuke Tanaka *Tokyo Institute of Technology, AIST* Secret Sharing with Statistical Privacy and Computational Relaxed Non-Malleability Tasuku Narita, Fuyuki Kitagawa, Yusuke Yoshida, Keisuke Tanaka *Tokyo Institute of Technology, NTT Secure Platform Laboratories*
KST 10:20 – 10:50 UTC 01:20 – 01:50	**Break Time**
KST 10:50 – 11:50 UTC 01:50 – 02:50	**Invited Talk 1** Designing the NIST post-quantum public-key candidate Saber Sujoy Sinha Roy *University of Birmingham*
KST 11:50 – 14:00 UTC 02:50 – 05:00	**Break Time (Lunch Time in Korea)**
KST 14:00 – 14:50 UTC 05:00 – 05:50	**Session 2: Constructions and Designs** A Sub-linear Lattice-based Submatrix Commitment Huang Lin, Yuguang Fang *Mercury's Wing & Suterusu project, University of Florida* PIPO: A Lightweight Block Cipher with Efficient Higher-Order Masking Software Implementations Hangi Kim, Yongjin Jeon, Giyoon Kim, Jongsung Kim, Bo-Yeon Sim, Dong-Guk Han, Hwajeong Seo, Seonggyeom Kim, Seokhie Hong, Jaechul Sung, Deukjo Hong *Kookmin University, Hansung University, Korea University, Jeonbuk National University*
KST 14:50 – 15:10 UTC 05:50 – 06:10	**Break Time**
KST 15:10 – 16:00 UTC 06:10 – 07:00	**Session 3: Efficient Implementations** Curve448 on 32-bit ARM Cortex-M4 Hwajeong Seo, Reza Azarderakhsh *Hansung University, Florida Atlantic University* Efficient Implementation of SHA-3 Hash Function on 8-bit AVR-based Sensor Nodes Youngbeom Kim, Hojin Choi, Seog Chung Seo *Kookmin University*

Thursday, (2020-12-03)	
KST 09:30 – 10:45 UTC 00:30 – 01:45	**Session 4: Security Analysis** Can a Differential Attack Work for an Arbitrarily Large Number of Rounds? Nicolas Courtois, Jean-Jacques Quisquater *University College London, UCL DICE/Crypto Group* Key Mismatch Attack on ThreeBears, Frodo and Round5 Jan Vacek, Jan Václavek *Thales* A New Non-random Property of 4.5-Round PRINCE Bolin Wang, Chan Song *Institute of Software Chinese Academy of Sciences*
KST 10:45 – 11:10 UTC 01:45 – 02:10	**Break Time**
KST 11:10 – 12:10 UTC 02:10 – 03:10	**Invited Talk 2** Tweakable Block Cipher-Based Cryptography Thomas Peyrin *Nanyang Technological University*
KST 12:15 – 14:00 UTC 03:15 – 05:00	**Break Time (Lunch Time in Korea)**
KST 14:00 – 15:00 UTC 05:00 – 06:00	**Invited Talk 3** Next Generation Cryptography Standards Lily Chen *NIST*
KST 15:00 – 15:20 UTC 06:00 – 06:20	**Break Time**
KST 15:20 – 16:10 UTC 06:20 – 07:10	**Session 5: Cryptography in Quantum Computer Age** (Quantum) Cryptanalysis of Misty schemes Aline Gouget, Jacques Patarin, Ambre Toulemonde *Thales DIS, University of Versailles* An Efficient Authenticated Key Exchange from Random Self-Reducibility on CSIDH Tomoki Kawashima, Katsuyuki Takashima, Yusuke Aikawa, Tsuyoshi Takagi *The University of Tokyo, Mitsubishi Electric Corporation*

Friday, (2020-12-04)	
KST 09:30 – 10:20 UTC 00:30 – 01:20	**Session 6: Artificial Intelligence and Cryptocurrency** Generative Adversarial Networks based Pseudo-Random Number Generator for Embedded Processors Hyunji Kim, Yongbeen Kwon, Minjoo Sim, Sejin Lim, Hwajeong Seo *Hansung University* A RDBMS-based Bitcoin Analysis System Hyunsu Mun, Youngseok Lee, Soohyun Kim *Chungnam National University*
KST 10:20 – 10:40 UTC 01:20 – 01:40	**Break Time**
KST 10:40 – 11:30 UTC 01:40 – 02:30	**Session 7: Fault and Side-Channel Attack** Federated Learning in Side-Channel Analysis Huanyu Wang, Elena Dubrova *KTH Royal Institute of Technology* Differential Fault based Key Recovery Attacks on TRIAD Iftekhar Salam, Kim Young Law, Luxin Xue, Wei-Chuen Yau *Xiamen University Malaysia*
	Farewell

* Program could be changed.