ASIACRYPT 2011

Rump Session

19:00 – 19:05 **Opening**
Orr Dunkelman

Announcements

19:05 – 19:15 **ASIACRYPT 2011 Statistics**
Dong Hoon Lee

19:15 – 19:17 **PAIRING 2012 Announcement**
Michel Abdalla, Tanja Lange, and Michael Naehrig

19:17 – 19:19 **Second Bar-Ilan Winter School**
Nir Bitansky on behalf of Claudio Orlandi

19:19 – 19:24 **The Ecological Crisis Facing Modern Cryptology**
BS, JTM, YLC

Constructions

19:24 – 19:29 **Generic Construction of Chosen Ciphertext Secure Proxy Re-Encryption**
Goichiro Hanaoka, Yutaka Kawai, Noboru Kunihiro, Takahiro Matsuda, Jian Weng, Rui Zhang, and Yunlei Zhao

19:29 – 19:37 **Towards Practical Oblivious RAM**
Emil Stefanov, Elaine Shi, and Dawn Song

19:37 – 19:42 **Construction and Security of a Non-Algebraic Tiny and Extensible Hash Function**
Hirotake Yaguchi

19:42 – 19:50 **Publicly Verifiable Delegation of Computation**
Papamanthou Charalampos, Elaine Shi, and Roberto Tamassia

Destructions

19:50 – 19:53 **Advances in System Solving**
Chen-Mou Cheng, Bo-Yin Yang, Tung Chou, Ruben Niederhagen, Yun-Ju Huang, Ming-Shing Chen

19:53 – 20:00 **Amplified Bicliques and Full IDEA**
Dmitry Khovratovich, Gaëtan Leurent, and Christian Rechberger

20:00 – 20:05 **Practical Collisions in Round-Reduced Keccak**
Itai Dinur, Orr Dunkelman, and Adi Shamir

20:05 – 20:11 **Clockwise Collision Analysis — Overlooked Side-Channel Leakage Inside Your Measurements**
Yang Li, Daisuke Nakatsu, Qi Li, Kazuo Ohta, and Kazuo Sakiyama

20:11 – 20:15 **Best Rump Session Presentation Award(s)**