The 12th Workshop among Asian Information Security Labs (WAIS 2020)

Program

Feb. 21.

10:00-12:05 Cryptography

C-1. Computationally Secure Verifiable Secret Sharing Scheme
Takato Imai (Tokyo Univ. of Sci.), Keiichi Iwamura (Tokyo Univ. of Sci.)

C-2. Improved CRT-RSA Secret Key Recovery Method from Sliding Window Leakage
Kento Oonishi (Univ. Tokyo), Xiaoxuan Huang (Univ. Tokyo),
Noboru Kunihiro (Univ. Tsukuba),

C-3. A Constant-time Algorithm of CSIDH keeping Two Points
Hiroshi Onuki (Univ. Tokyo), Yusuke Aikwa (Mitsubishi),
Tsutomu Yamazaki (Kyushu Univ.), Tsuyoshi Takagi (Univ. of Tokyo),

C-4. Path-finding Algorithms in LPS/LPS-type Ramanujan Graphs
Hyungrok Jo (Univ. Tsukuba)

C-5. Hybrid meet-in-the-middle attacks for the isogeny path-finding problem
Yasuhiko Ikematsu (Kyushu University)

12:05-14:00 Lunch

14:00-14:50 Network Security

NS-1. Lightweight Misbehavior Detection Management of Embedded IoTDevices in Medical Cyber Physical Systems
Philip Astillo (Soonchunhyang Univ.), Daniel Gerbi Duguma (Soonchunhyang Univ.),
Gaurav Choudhary (Soonchunhyang Univ.), Ilsun You (Soonchunhyang Univ.)

NS-2. 5G wireless P2MP backhaul security protocol with Formal Verification
Jiyoon Kim (Soonchunhyang Univ.), Hoonyong Park (Soonchunhyang Univ.),
Ilsun You (Soonchunhyang Univ.)

14:50-15:15 Coffee Break

15:15-16:30 AI Security

AI-1. Video Tampering Detection Using Machine Learning
Hiroki Ueda (Tokyo Univ. of Sci.), Hyunho Kang (NIT, Tokyo College),
Keiichi Iwamura (Tokyo Univ. of Sci.)

AI-2. Digital Watermarking Using Machine Learning
Hiroyuki Imada (Tokyo Univ. of Sci.), Hyunho Kang (NIT, Tokyo College),
Naoto Kawamura (KTL), Keiichi Iwamura (Tokyo Univ. of Sci.)

AI-3. Power and Limitation of Cyber Attack with Adversarial examples
Kouichi SAKURAI (Kyushu Univ.)

16:30-17:30 WAIS-2020 Steering Committee Meeting and Discussion about WAIS-2021 plan

17:30-20:00 Banquet