LIST OF ACCEPTED PAPERS[1]

ISC2017

Rate-One AE with Security under RUP. Shoichi Hirose (University of Fukui, Japan), Yu Sasaki and Kan Yasuda (NTT Secure Platform Laboratories, Japan)

Contactless Access Control based on Distance Bounding. Handan Kılınç and Serge Vaudenay (EPFL, Switzerland)

A Differentially Private Encryption Scheme. Carlo Brunetta, Bei Liang (Chalmers University of Technology, Sweden), Christos Dimitrakakis (Chalmers University / University of Lille / Harvard University, Sweden) and Aikaterini Mitrokotsa (Chalmers University of Technology, Sweden)

Low-level Attacks in Smart-card Bitcoin Wallets. Andriana Gkaniatsou, Myrto Arapinis and Aggelos Kiayias (School of Informatics, University of Edinburgh, UK)

Visualization of Intrusion Detection Alarms collected across Multiple Networks. Boyeon Song, Sang-Soo Choi, Jangwon Choi and Jungsuk Song (Korea Institute of Science and Technology Information, South Korea)

Watermarking Public-key Cryptographic Functionalities and Implementations. Foteini Baldimtsi (George Mason University, USA), Aggelos Kiayias (University of Edinburgh and IOHK, UK) and Katerina Samari (National and Kapodistrian University of Athens, Greece)

Harvesting Smartphone Privacy through Enhanced Juice Filming Charging Attacks. Weizhi Meng (DTU, Denmark), Fei Fei (CityU HK, Hong Kong), Wenjuan Li (CityU HK, Hong Kong) and Man Ho Au (PolyU HK, Hong Kong)

T-MAC: Protecting Mandatory Access Control System Integrity from Malicious Execution Environment on ARM-based Mobile Devices. Diming Zhang, Liangqiang Chen, Hao Wu, Fei Xue and Hao Huang (Nanjing University, China)

Homomorphic-policy attribute-based key encryption mechanisms. Jérémy Chotard (XLIM, University of Limoges, CNRS and ENS, CNRS, INRIA, PSL Research University, Paris, France),

Duong Hieu Phan (XLIM, University of Limoges, CNRS, France) and David Pointcheval (ENS, CNRS, INRIA, PSL Research University, Paris, France)

An Improved SAT-based Guess-and-Determine Attack on the Alternating Step Generator. Oleg Zaikin and Stepan Kochemazov (ISDCT SB RAS, Russia)

Zero-Knowledge Password Policy Check from Lattices. Khoa Nguyen, Benjamin Hong Meng Tan and Huaxiong Wang (Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore)

[1] In in no particular order.

Run-time Verification for Observational Determinism Using Dynamic Program Slicing. Mohammad Ghorbani and Mehran S. Fallah (Amirkabir University of Technology, Iran)

Generic Forward-Secure Key Agreement Without Signatures. Cyprien Delpech de Saint Guilhem, Nigel Smart and Bogdan Warinschi (University of Bristol, UK)

On Subfield Lattice Attack against overstretched NTRU revisited. Dung Hoang Duong, Masaya Yasuda (Kyushu University, Japan) and Tsuyoshi Takagi (Kyushu University and The University of Tokyo, Japan)

Droid Mood Swing (DMS): Automatic security modes based on the context. Md Shahrear Iqbal and Mohammad Zulkernine (School of Computing, Queen's University, Kingston, Ontario, Canada)

Improving Gait Cryptosystem Security Using Gray Code Quantization and Linear Discriminant Analysis. Lam Tran (Chonnam National University, South Korea), Thang Hoang (Oregon State University, USA), Thuc Nguyen (Ho Chi Minh University of Science, Vietnam) and Deokjai Choi (Chonnam National University, South Korea)

Nightingale: Translating Embedded VM Code in x86 Binary Executables. Haijiang Xie (Shanghai Jiao Tong University and Keen Security Lab of Tencent, China), Juanru Li, Yuanyuan Zhang and Dawu Gu (Shanghai Jiao Tong University, China)

Enforcing ACL Access Control on Android Platform. Xiaohai Cai (University of Chinese Academy of Sciences and Institute of Information Engineering, Chinese Academy of Sciences and Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, China), Xiaozhuo Gu, Yuewu Wang, Quan Zhou (Institute of Information Engineering, Chinese Academy of Sciences and Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, China) and Zhenhuan Cao (Gansu Information Center, China)

Curtain: Keep your hosts away from USB attacks. Jianming Fu (Key laboratory of Aerospace Information Security and Trusted Computing, Wuhan University, China), Jianwei Huang and Lanxin Zhang (School of Computer Science, Wuhan University, China)

Constant-size Signatures with Tighter Reduction from CDH Assumption. Kaisei Kajita, Kazuto Ogawa (Japan Broadcasting Corporation, Japan) and Eiichiro Fujisaki (Japan Advanced Institute of Science and Technology, Japan)

Improved Automatic Search Tool for Related-Key Differential Characteristics on Byte-Oriented Block Ciphers. Li Lin, Wenling Wu and Yafei Zheng (Institute of Software, Chinese Academy of Sciences and University of Chinese Academy of Science, China)

Improving Passwords Guessing Using Byte Pair Encoding. Xingxing Wang (School of Cyberspace Security, Beijing University Of Posts And Telecommunications, China), Dakui Wang, Xiaojun Chen, Rui Xu, Jinqiao Shi and Li Guo (Institute of Information Engineering, Chinese Academy of Science, China).

How To Make Information-Flow Analysis Based Defense Ineffective: An ART Behavior-Mask Attack. Xueyi Yang (School of Cyber Security, University of Chinese Academy of Sciences and State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences and Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, China), Limin Liu, Lingchen Zhang, Weiyu Jiang (State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences and Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, China) and Shiran Pan (School of Cyber Security, University of Chinese Academy of Sciences and State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences and Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, China)

Automated Analysis of Accountability. Alessandro Bruni, Rosario Giustolisi and Carsten Schuermann (IT University of Copenhagen, Denmark).

Efficient Masking of ARX-Based Block Ciphers Using Carry-Save Addition on Boolean Shares. Daniel Dinu, Johann Großschädl and Yann Le Corre (University of Luxembourg, Luxembourg).