The 12th
International
Conference on

Provable Security

25-28 October 2018
Jeju Island, Republic of Korea

Table of Contents

ProvSec 2018 is organized by

- Institute of Cybersecurity and Cryptology (iC^2), University of Wollongong, Australia
- Laboratory of Mobile Internet Security, Soonchunhyang University, Korea

ProvSec 2018 is in association with

- KIISC Research Group on 5G Security
- Information Education and Security Laboratory, Jeju National University, Korea
- Innovative Information Science & Technology Research Group, Korea

1. Welcome to ProvSec 2018

ProvSec 2018 is organized by the Institute of Cybersecurity and Cryptology at the University of Wollongong and the Laboratory of Mobile Internet Security at Soonchunhyang University.

The first ProvSec conference was started in Wollongong, Australia in 2007. The series of ProvSec conferences were then held successfully in Shanghai, China (2008), Guangzhou, China (2009), Malacca, Malaysia (2010), Xian, China (2011), Chengdu, China (2012), Malacca, Malaysia (2013) , Hong Kong, China (2014), Kanazawa Japan (2015), Nanjing, China (2016) and Xian, China (2017). This was the first ProvSec held in Korea. This year we received 48 submissions of high quality from 19 countries.

Among the accepted regular papers, the paper that received the highest weighted review mark was given the Best Paper Award: *"Security Notions for Cloud Storage and Deduplication"* by Colin Boyd, Gareth T. Davies, Kristian Gjøsteen, Håvard Raddum and Mohsen Toorani.

The program also included an invited talk presented by Prof. Jung Hee Cheon from Seoul National University, Korea, titled *"Recent Development of Homomorphic Encryptions and Their Applications".*

ProvSec Workshop 2018 is jointly held with the conference. Twelve selected papers will be presented during the workshop.

We deeply thank all the authors of the submitted papers. We also greatly appreciate time and effort that the Program Committee members and external reviewers put to evaluate and select the papers for the program. Our gratitude extends to our sponsors - Jeju National University, Korea and Innovation Information Science and Technology Research Group, Korea. We are also grateful to the team at Springer for their continuous support of the conference and for their assistance in the production of the conference proceedings.

October 2018

Ilsun You
Kyung Hyune Rhee
Joonsang Baek
Willy Susilo

2. ProvSec 2018 Conference Organization

General Chairs

Ilsun You	Soonchunhyang University, Korea
Kyung Hyune Rhee	Pukyung National University, Korea

Program Chairs

Joonsang Baek	University of Wollongong, Australia
Willy Susilo	University of Wollongong, Australia

Publication Chair

Jongkil Kim	University of Wollongong, Australia

Organization Chair

Namje Park	Jeju National University, Korea

Program Committee

Elena Andreeva	K.U. Leuven, Belgium
Man Ho Au	The Hong Kong Polytechnic University, Hong Kong
Donghoon Chang	IIIT-Delhi, India
Jie Chen	East China Normal University, China
Liqun Chen	University of Surrey, UK
Xiaofeng Chen	Xidian University, China
Cheng-Kang Chu	Huawei, Singapore
Bernardo David The	Tokyo Institute of Technology, Japan
Jean Paul Degabriele	TU Darmstadt, Germany
Robert Deng	Singapore Management University, Singapore
Keita Emura	NICT, Japan
Zekeriya Erkin	TU Delft, Netherlands
Jinguang Han	University of Surrey, UK
Ryo Kikuchi	NTT, Japan
Jongkil Kim	University of Wollongong, Australia
Hyung Tae Lee	Chonbuk National University, Korea
Jooyoung Lee	KAIST, Korea
Joseph Liu	Monash University, Australia
Bernardo Magri	Friedrich-Alexander-University, Germany
Barbara Masucci	University of Salerno, Italy
Bart Mennink Radboud	University, Netherlands
Chris Mitchell	Royal Holloway, University of London, UK
Kirill Morozov	University of North Texas, USA
Khoa Nguyen	Nanyang Technological University, Singapore
Abderrahmane Nitaj	Université de Caen Normandie, France
Josef Pieprzyk	CSIRO/Data61, Australia

Kouichi Sakurai	Kyushu University, Japan
Rainer Steinwandt Florida	Atlantic University, USA
Chunhua Su	Osaka University, Japan
Katsuyuki Takashima	Mitsubishi Electric, Japan
Atsushi Takayasu The	University of Tokyo, Japan
Qiang Tang	New Jersey Institute of Technology, USA
Joseph Tonien	University of Wollongong, Australia
Damien Vergnaud	ENS, France
Shota Yamada	AIST, Japan
Chung-Huang Yang	National Kaohsiung Normal University, Taiwan
Guomin Yang	University of Wollongong, Australia
Xun Yi	RMIT University, Australia
Yong Yu	Shaanxi Normal University, China
Tsz Hon Yuen	The University of Hong Kong, Hong Kong
Aaram Yun	UNIST, Korea

Workshop Organization

Program Co-Chairs

Jongkil Kim	University of Wollongong, Austraila
Joonsang Baek	University of Wollongong, Austraila

Program Committee

Taekyong Kwon	Yonsei University, South Korea
Jong-Hyouk Lee	Sangmyung University, South Korea
Nan Li	University of Newcastle, Australia
Deepak Puthal	University of Technology Sydney, Australia
Vishal Sharma	Soonchunhyang University, South Korea
Pairat Thorncharoensri	University of Wollongong, Australia
Ilsun You	Soonchunhyang University, South Korea

3. ProvSec 2018 Program

2018-10-25 (Thursday) - ProvSec 2018 Workshop

Standard duration of presentation: 15 minutes
Workshop Venue: Seminar Room, 8th Floor, Ocean Grand Hotel

12:30 - 17:25	Registration
13:20 - 13:30	Opening
13:30 - 15:00	Workshop Session I: General ICT Framework and Security (Chair: Ilsun You) A Study of Distributed Mobility Management for 5G Networks Soohyun Kwon (Soonchunhyang University), Jiyoon Kim (Soonchunhyang University), Takshi Gupta (Soonchunhyang University) and Ilsun You (Soonchunhyang University) A Framework for Cloud IVS Management through FedRAMP Analysis Jiyeon Kim (Jeju National University) and Namje Park (Jeju National University) Intelligent Information Technology-based ICT Education and Creativity Education Develop Core Competencies Yujin Jung (Jeju National University), Namje Park (Jeju National University) and Heuipil Kim (Jeju National University) The Rigidity of Rectangular Frameworks Keunbae Choi(Jeju Naltional University) and Namje Park (Jeju National University) Strong Designated Verifier Signcryption Scheme Neetu Sharma (PRS University), Rajeev Anand Sahu (Universite Libre de Bruxelles), Vishal Saraswat (IIT Jammu), Gaurav Sharma (Universite Libre de Bruxelles), Veronika Kuchta (Monash University), Olivier Markowitch (Universite Libre de Bruxelles)
15:00 - 15:30	Coffee Break
15:30 - 17:30	Workshop Session II: Security and Applications (Chair: Jongkil Kim) Securely outsourcing machine learning with multiple users Ping Li (Guangzhou University), Hongyang Yan (Nankai University), Chong-Zhi Gao (Guangzhou University), Yu Wang (Guangzhou University), Liaoliang Jiang (Guangzhou University) and Yuefang Huang (Guangzhou University) Lattice-Based Simulatable VRFs: Challenges and Future Directions Carlo Brunetta (Chalmers University of Technology), Bei Liang (Chalmers

	University of Technology) and Aikaterini Mitrokotsa (Chalmers University of Technology) An SDN-based Secure Mobility Model for UAV-Ground Communications Rajesh Kumar (TIET), Mohd. Abuzar Sayeed (TIET), Vishal Sharma (Soonchunhyang University), Ilsun You (Soonchunhyang University) Expressive Ciphertext-Policy Attribute-Based Encryption with Fast Decryption Hikaru Tsuchida (NEC Corporation), Takashi Nishide (University of Tsukuba) and Eiji Okamoto (University of Tsukuba) Achieving Strong Security and Member Registration for Lattice-based Group Signature Scheme with Verifier-local Revocation Maharage Nisansala Sevwandi Perera (Saitama University) and Takeshi Koshiba (Waseda University) A Type-based Formal Specification for Cryptographic Protocols Paventhan Vivekanandan (Indiana University Bloomington) A Novel Non-Interactive Multi-party Key Exchange from Homomorphic Encryption Rakyong Choi (KAIST) and Kwangjo Kim (KAIST)
19:00 - 21:00	Welcome Reception Venue: Spanish Hamdeok

2018-10-26 (Friday) – ProvSec 2018 Conference

Standard duration of presentation: Full Paper – 30 minutes, Short Paper – 15-20 minutes
Conference Venue: Seminar Room, 8th Floor, Ocean Grand Hotel

08:30 - 17:25	Registration
09:00 - 09:30	Opening
09:30 - 10:30	Keynote (Chair: Joonsang Baek) Recent Development of Homomorphic Encryptions and Their Applications Prof. Jung Hee Cheon (Seoul National University)
10:30 - 11:00	Coffee Break
11:00 - 12:30	Conference Session: Foundation 1 (Chair: Kouichi Sakurai) On the Leakage of Corrupted Garbled Circuits Aurélien Dupin (Thales Communications & Security), David Pointcheval (DIENS, École normale supérieure) and Christophe Bidan (CentraleSupélec)

	Secure Outsourcing of Cryptographic Circuits Manufacturing Giuseppe Ateniese (Stevens Institute of Technology), Aggelos Kiayias (The University of Edinburgh), Bernardo Magri (Friedrich-Alexander-Universität Erlangen-Nürnberg), Yiannis Tselekounis (The University of Edinburgh) and Daniele Venturi (Sapienza University of Rome) Verifiable Homomorphic Secret Sharing Georgia Tsaloli (Chalmers University of Technology), Bei Liang (Chalmers University of Technology) and Aikaterini Mitrokotsa (Chalmers University of Technology)
12:30 - 13:30	Lunch
13:30 - 15:00	Conference Session: Public Key Encryption 1 (Chair: Gareth T. Davies) A CCA-Secure Collusion-Resistant Identity-Based Proxy Re-Encryption Scheme Arinjita Paul (Indian Institute of Technology Madras), Varshika Srinivasavaradhan (Thiagarajar College of Engineering), S. Sharmila Deva Selvi (Indian Institute of Technology Madras) and Chandrasekaran Pandurangan (Indian Institute of Technology Madras) Multivariate Encryption Schemes Based on the Constrained MQ Problem Token-Based Multi-Input Functional Encryption Takanori Yasuda (Okayama University of Science) Token-Based Multi-Input Functional Encryption Nuttapong Attrapadung (National Institute of Advanced Industrial Science and Technology), Goichiro Hanaoka (National Institute of Advanced Industrial Science and Technology), Takato Hirano (Mitsubishi Electric Corporation), Yutaka Kawai (Mitsubishi Electric Corporation), Yoshihiro Koseki (Mitsubishi Electric Corporation) and Jacob C. N. Schuldt (National Institute of Advanced Industrial Science and Technology)
15:00 - 15:30	Coffee Break
15:30 - 16:30	Conference Session: Public Key Encryption 2 (Chair: Kyung Hyune Rhee) On the CCA2 Security of McEliece in the Standard Model Edoardo Persichetti (Florida Atlantic University) Efficient Attribute-Based Encryption with BlackBox Traceability Shengmin Xu (University of Wollongong), Guomin Yang (University of Wollongong), Yi Mu (Fujian Normal University) and Ximeng Liu (Fuzhou University)
16:30 - 17:30	Conference Session: Digital Signature 1 (Chair: Britta Hale) A Code-Based Linkable Ring Signature Scheme Pedro Branco (IST-Universidade de Lisboa) and Paulo Mateus (IST-Universidade de Lisboa)

	Towards Static Assumption Based Cryptosystem in Pairing Setting: Further Applications of DejaQ and Dual-Form Signature Sanjit Chatterjee (Indian Institute of Science, Bangalore) and R. Kabaleeshwaran (Indian Institute of Science, Bangalore)
19:00 - 21:00	Banquet and Best Paper Award Ceremony Venue: 8th Floor, Ocean Grand Hotel

2018-10-27 (Saturday) - ProvSec 2018 Conference

08:30 - 15:25	Registration
09:00 - 10:30	Conference Session: Digital Signature 2 (Chair: Paulo Mateus) Digital Signatures from the Middle-Product LWE Ryo Hiromasa (Mitsubishi Electric) Generic Double-Authentication Preventing Signatures and a Post-Quantum Instantiation David Derler (Graz University of Technology), Sebastian Ramacher (Graz University of Technology) and Daniel Slamanig (AIT Austrian Institute of Technology) A Simpler Construction of Identity-Based Ring Signatures from Lattices Gongming Zhao (Anhui University) and Miaomiao Tian (Anhui University)
10:30 - 11:00	Coffee Break
11:00 - 12:30	Conference Session: Applications (Chair: Rajesh Kumar) Modeling Privacy in WiFi Fingerprinting Indoor Localization Zheng Yang (Singapore University of Technology and Design) and Kimmo Järvinen (University of Helsinki) Security Notions for Cloud Storage and Deduplication Colin Boyd (Norwegian University of Science and Technology), Gareth T. Davies (Norwegian University of Science and Technology), Kristian Gjøsteen (Norwegian University of Science and Technology), Håvard Raddum (Simula@UiB) and Mohsen Toorani (University of Bergen) Forward Secrecy for SPAKE2 Jose Becerra (University of Luxembourg), Dimiter Ostrev (University of Luxembourg) and Marjan Skrobot (University of Luxembourg)
12:30 - 13:30	Lunch
13:30 - 15:00	Conference Session: Foundation 2 (Chair: Edoardo Persichetti) Location-Proof System Based on Secure Multi-Party Computations Aurélien Dupin, Jean-Marc Robert (École de Technologie Supérieure) and Christophe Bidan (CentraleSupélec)

	On the Hardness of Learning Parity with Noise over Rings Shuoyao Zhao (Shanghai Jiao Tong University), Yu Yu (Xi'an University of Posts and Telecommunications) and Jiang Zhang (State Key Laboratory of Cryptology) Single Private-Key Generator Security Implies Multiple Private-Key Generators Security Atsushi Fujioka (Kanagawa University) and Kazuki Yoneyama (Ibaraki University)
15:00 - 15:30	Coffee Break
15:30 - 16:30	Conference Session: Symmetric Cryptography (Chair: Jongkil Kim) A Generic Construction of Sequential Aggregate MACs from Any MACs Shingo Sato (Yokohama National University), Shoichi Hirose (University of Fukui) and Junji Shikata (Yokohama National University) Length-Preserving Encryption Based on Single-key Tweakable Block Cipher Xiangyang Zhang (Shanghai Jiao Tong University), Yaobin Shen (Shanghai Jiao Tong University), Hailun Yan (Shanghai Jiao Tong University), Ying Zou (Shanghai Jiao Tong University), Ming Wan (Shanghai Jiao Tong University), Zheyi Wu (Shanghai Jiao Tong University) and Lei Wang (Shanghai Jiao Tong University)
16:30 - 17:50	Conference Session: Short Papers (Chair: Vishal Sharma) User-Mediated Authentication Protocols and Unforgeability for Key Collision Britta Hale (Naval Postgraduate School) BAdASS: Preserving Privacy in Behavioural Advertising with Applied Secret Sharing Leon J. Helsloot (Delft University of Technology), Gamze Tillem (Delft University of Technology) and Zekeriya Erkin (Delft University of Technology) Signcryption with Quantum Random Oracles Shingo Sato (Yokohama National University) and Junji Shikata (Yokohama National University) Formal Treatment of Verifiable Privacy-Preserving Data-Aggregation Protocols Satoshi Yasuda (Mitsubishi Electric), Yoshihiro Koseki (Mitsubishi Electric), Yusuke Sakai (National Institute of Advanced Industrial Science and Technology), Fuyuki Kitagawa (Tokyo Institute of Technology), Yutaka Kawai (Mitsubishi Electric) and Goichiro Hanaoka (National Institute of Advanced Industrial Science and Technology)

2018-10-28 (Sunday) - ProvSec 2018 Conference

09:00 - 09:30	Steering Committee Meeting
10:00 - 11:30	Other Local Committee Meetings
11:30 - 12:00	Adjourn