Guest Editorial: Special Issue on "15th Asia Joint Conference on Information Security, AsiaJCIS 2020"

Yu-Chi Chen, Rui Tanabe, Yujue Wang, Huy Kang Kim

Information security is a multidisciplinary area that addresses the development and implementation of security mechanisms in order to protect information systems with specific purposes against potential attacks or threats. The security goal can be defined for each type of attacks. The currently relevant set of security goals includes confidentiality, integrity, availability, privacy, authenticity and trustworthiness, non-repudiation, accountability and auditability. However, with the rapid global penetration of network, different models are considered to design new solutions to realizing information security (e.g., in IoT or distributed scenarios). This attracts lots of attention to work on information security research on modern architecture of information systems. Very recently, the AI techniques have joined this area and also acted as a double-edged sword in realizing attacks and defenses.

The main purpose of this special issue is to publish selected papers with high-quality from "15th Asia Joint Conference on Information Security (AsiaJCIS 2020)." In this special issue, we focus mainly on cryptography, network security, system security, and application security. We are interested in the novel ideas, advanced techniques, comparative analysis of different methodologies, detailed surveys, and technical reviews on all aspects of cooperative communications and mechanisms in information security. This special issue also covers industrial applications and academic research contributions, and totally includes three papers that are the extended version from their conference papers.

The paper entitled "Linear and Lossy Identification Schemes derive Tightly Secure Multisignatures" by Masayuki Fukumitsu (Hokkaido Information University) and Shingo Hasegawa (Tohoku University), presents a generic construction of multisignature schemes which is tightly secure in the plain public key and random oracle model. The construction can capture the known tightly secure multisignature schemes. The generic construction is derived from the identification (ID) scheme which has two properties called the linearity and the lossiness. It also proposes a new property of ID schemes, called the difference soundness, and show that the combination of the linearity and the difference soundness implies the lossiness. The multisignature scheme admits multiple signers in the signature generation. The signers compute a single signature on a single common message in an interactive manner. The resulting signature ensures that the signers having a corresponding public key used in the verification participated in the signature generation. This feature yields the advantage for the multisignature scheme in the case where each signer issues an ordinary signature individually because the size of a multisignature can be less than the total size of individual signatures by signers. Thus, the multisignature scheme is considered as an attractive building block to develop a resource-constrained technology such as the IoT and the blockchain.

The paper entitled "Effective Classification for Multi-modal Behavioral Authentication on Large-Scale Data" by Shuji Yamaguchi, Hidehito Gomi (Yahoo Japan), Ryosuke Kobayashi, and Rie Shigetomi Yamaguchi (University of Tokyo), proposes an effective classification algorithm for machine learning to achieve higher performance for multimodal behavioral authentication systems. The main algorithm uses a multiclass classification scheme that has a smaller number of classes than the number of users stored in the dataset. The paper also proposes metrics, the self-mix-classified rate, other-single-classified rate, and equal-classified rate, for use with the proposed algorithm to determine an optimal number of classes for behavioral authentication. The experiments using a large-scale dataset of activity histories that are stored when 100,000 users use commercial smartphone-applications to analyze performance measures such as false rejection rate, false acceptance rate, and equal error rate obtained with the proposed algorithm. It has achieved higher performance than the previous ones.

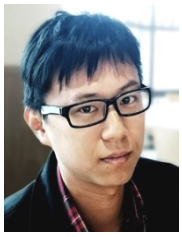
The paper entitled "A Generic Construction of Predicate Proxy Key Re-encapsulation Mechanism" by Yi-Fan Tseng, Zi-Yuan Liu, Raylin Tso (National Chengchi University), affirmatively solves this by proposing two generic constructions that can transform any linear predicate key encapsulation mechanism (PKEM) or any linear PE scheme to a predicate proxy key re-encapsulation mechanism (PPKREM). The proposed construction is payload hiding of second/ first-level ciphertext (i.e., original/re-encapsulation ciphertext) secure in the standard model, if the

*Corresponding Author: Yu-Chi Chen; E-mail: wycchen@saturn.yzu.edu.tw

underlying PKEM satisfies indistinguishability under chosen-ciphertext attacks (IND-CCA). Then, since secure key encapsulation mechanism (KEM) can be used as a building block to construct public key encryption, i.e., combining with a secure symmetric encryption scheme, it can be applied to construct a secure proxy re-encryption.

As the Guest Editors of this special issue, we would like to thank all reviewers and authors in this special issue for their efforts in making helpful comments and significant contributions. Finally, our special thanks go to Prof. Han-Chieh Chao and Chi-Yuan Chen, the (Executive) Editor-in-Chiefs of JIT, for their encouragement and support to publish this special issue and to Ms. Sharon Chang, the Assistant of JIT, for her professional help during the preparation of this special issue.

Guest Editors



Yu-Chi Chen received the B.S., M.S., and Ph.D. degrees from Department of Computer Science and Engineering, National Chung-Hsing University, Taiwan, in 2008, 2009, and 2014 respectively. In 2013, he was a visiting scholar at Department of Electrical Engineering, University of Washington. He was a postdoctoral fellow at the Institute of Information Science, Academia Sinica, Taiwan from 2014 to 2017. He is currently an associate professor at Department of Computer Science and Engineering, Yuan Ze University, Taiwan. His research interests include cryptography, information security, blockchain, and privacy preserving machine learning. He has received Graduate Student Study Abroad Program from Taiwan National Science Council in 2012, Student Academic Publication Award from National Chung Hsing University in 2013, Academia Sinica Postdoctoral Fellowship from Academia Sinica in 2015, Best Journal Papers Award from Association for Algorithms and Computation Theory in 2017, Short-term Visiting Program for Domestic Scholars from Academia Sinica in 2018, Project for Excellent Junior Research Investigators from Taiwan Ministry of Science and Technology in 2020, and Innovation in Teaching Award and Young Scholar Research Award from the Yuan Ze University in 2020. He is currently an Associate Editor of IEEE Access and Journal of Information Technology

Rui Tanabe received his Ph.D. in information sciences from Yokohama National University in 2017. After working at Yokohama National University as a project assistant professor, Dr. Tanabe is currently working as a project associate professor at Yokohama National University. His research interests include information security and network security. He received the Yamashita Memorial Research Award from IPSJ in 2017.

Yujue Wang received the Ph.D. degrees from the Wuhan University and City University of Hong Kong under the joint Ph.D. program. He was a Research Fellow with the Secure Mobile Centre of Singapore Management University and the Department of Computing of The Hong Kong Polytechnic University, and was an Associate Professor with the Guilin University of Electronic Technology. He is currently a Senior Research Fellow with the Hangzhou Innovation Institute of Beihang University. His current research interests include applied cryptography and cloud computing security.

Huy Kang Kim received a B.S. degree in Industrial Management, M.S. degree in Industrial Engineering and Ph.D. degree in Industrial and System Engineering in Korea Advanced Institute of Science and Technology (KAIST), Republic of Korea. He is a serial entrepreneur; he founded A3 Security Consulting in 1999 and AI Spera, the data-driven cyber threat intelligence service company in 2017. Currently, he is a professor in the School of Cybersecurity, Korea University. His recent research is focused on anomaly detection in the intelligent transportation system, online gaming and internet banking by using data analytics and machine learning techniques.