Message from the Guest Editors

Guomin Yang¹ · Willy Susilo¹ · Yi Mu¹

Published online: 25 January 2016
© Springer-Verlag Berlin Heidelberg 2016

This special issue of the International Journal of Information Security includes 6 papers selected from the 26 full papers accepted by the 19th Australasian Conference on Information Security and Privacy (ACISP 2014) held at the University of Wollongong, Australia, during July 7–9, 2014. Papers included in this special issue are selected based on the comments and feedbacks from the conference Program Committee. Each paper contains substantial additional content compared with the conference version and has undergone another round of review in order to ensure high quality. We would like to thank all the authors and reviewers who have contributed to this special issue.

In the paper *Secure Three-Party Computational Protocols for Triangle Area*, which received the “Best Student Paper” in ACISP 2014, Liu et al. addressed a specific secure multi-party computation (MPC) problem of computing the area of a triangle among three parties, each of whom has the coordinate of one vertex of the triangle and does not want to reveal it to other parties. Their proposed protocols used a simpler assumption than that of the previous MPC protocols and employed a novel technique named “pseudorandom-then-rounding” to solve the problem.

In the paper *Sakai–Ohgishi–Kasahara Identity-Based Non-Interactive Key Exchange Revisited and More*, Chen et al. revisited the Sakai–Ohgishi–Kasahara (SOK) identity-based non-interactive key exchange (IB-NIKE) scheme.

They first improved the previous security analysis for the SOK IB-NIKE scheme in the random oracle model by giving a tighter reduction. Then they applied the meta-reduction technique to show that the SOK scheme is unlikely to be proven secure under the computational bilinear Diffie–Hellman (CBDH) assumption without programming the random oracle. Moreover, in the standard model, the authors showed how to instantiate the random oracle in the SOK scheme with a concrete hash function from admissible hash functions (AHFs) and indistinguishability obfuscation.

In the paper *Practical Chosen Ciphertext Secure Hierarchical Identity-Based Broadcast Encryption*, Liu et al. focused on the construction of practical Hierarchical Identity-Based Broadcast Encryption (HIBBE) with semantic security against adaptively chosen ciphertext attacks (CCA2) in the standard model. They first proposed a CPA-secure HIBBE scheme on prime-order bilinear groups and then proposed a new conversion technique to convert the basic scheme into a CCA2-secure scheme. The performance analysis and experiment show that their scheme is much more efficient than the previous HIBBE schemes.

In the paper *On Selection of Samples in Algebraic Attacks and a New Technique to Find Hidden Low Degree Equations*, Susil et al. studied the way of selecting samples in algebraic attacks against block ciphers. They introduced a strategy for selecting the plaintexts and demonstrated its strength by breaking reduced-round KATAN32, LBlock and SIMON.

In the paper *Strongly Simulation-Extractable Leakage-Resilient NIZK*, Wang and Tanaka defined the notion of strongly simulation-extractable (sSE) leakage-resiliency (LR) for non-interactive zero knowledge (NIZK) proof system. They also applied their sSE-LR-NIZK proof to construct the first fully leakage resilient signature scheme that is strongly existentially unforgeable.

✉ Willy Susilo
wsusilo@uow.edu.au

Guomin Yang
gyang@uow.edu.au

Yi Mu
ymu@uow.edu.au

¹ Centre for Computer and Information Security Research,
University of Wollongong, Wollongong, NSW 2522, Australia

In the paper *Efficient Attribute-Based Signature and Signcryption Realizing Expressive Access Structures*, Rao and Dutta presented two key-policy attribute-based signature (ABS) schemes with constant-size signature for expressive linear secret-sharing scheme (LSSS)-realizable monotone access structures. Their first scheme is a small-universe construction, while the second scheme supports a large uni-

verse of attributes. In addition, the authors also proposed a new attribute-based signcryption (ABSC) scheme for LSSS-realizable access structures with constant-size ciphertext. Their ABSC scheme achieves public verifiability of the ciphertext and is significantly more efficient than the previous schemes.