Preface

Tomoya Enokido*

Faculty of Business Administration,
Rissho University,
4-2-16, Osaki, Shinagawa,
Tokyo 1414-8602, Japan
Email: eno@ris.ac.jp
*Corresponding author

Xiaofeng Chen

School of Cyber Engineering,
Xidian University,
P.O. 106, Taibai South Road 2,
Xi'an 710071, China
Email: xfchen@xidian.edu.cn

Biographical notes: Tomoya Enokido received BE, ME and PhD degrees in Computers and Systems Engineering from Tokyo Denki University, Japan in 1997, 1999 and 2003, respectively. After working for NTT Data Corporation and Tokyo Denki University as a research associate, he joined Rissho University in 2005. He is now a full professor in the Faculty of Business Administration, Rissho University. His research interests include distributed systems and green computing. He is a member of IEEE and IPSJ.

Xiaofeng Chen received BS and MS in Mathematics from Northwest University, China in 1998 and 2000, respectively. He got PhD in Cryptography from Xidian University in 2003. Currently he is a Professor at Xidian University. His research interests include applied cryptography and cloud computing security. He has published over 100 research papers in refereed international conferences and journals. He is in the Editorial Board of IEEE Transactions on Dependable and Secure Computing (TDSC), Security and Communication Networks (SCN), Computing and Informatics (CAI), International Journal of Embedded Systems (IJES) etc. He has served as the program/general chair or program committee member in over 30 international conferences.

This special issue addresses recent advances and research findings on security services for Cloud computing. Each time more data and services from companies, businesses, institutions, and individuals are moved to Cloud computing platforms, security services have become an indispensable to ensure data integrity, business continuity and privacy. Indeed, an increasing number of threats have appeared to Cloud computing platforms requiring advances in encryption, authentication, data privacy, secure data access and transfer. For this special issue, we accepted six papers based on their quality and suitability.

In the first paper, Xie et al. propose a lattice-based searchable public-key encryption scheme for a designated tester. The proposed scheme is the first searchable public-key encryption scheme based on lattice hardness assumption (the LWE assumption). Moreover, the proposed scheme achieves the dPEKS ciphertexts indistinguishability and trapdoor indistinguishability. Therefore, the proposed scheme provides the strongest security level excluding inside KGAs.

In the second paper, Li et al. propose the concept of "multi-owner key-aggregate searchable encryption" scheme and its implementation, in which a user can only submit a trapdoor for querying the documents shared by multiple owners who only need to distribute an aggregate key for sharing massive data. The proposed scheme supports effective data sharing for both multiple owners and users by reducing unnecessary trapdoors which is hard for generating by mobile devices during the querying step.

In the third paper, Wang et al. first introduce a new cryptographic primitive: PRE+, which can be seen as the dual of traditional proxy re-encryption (PRE) primitive. Then, authors propose a scalable and controllable cloud data sharing framework for cloud users to provide secure cloud data sharing services in cloud storage.

In the fourth paper, Yang et al. introduce a searchable symmetric encryption scheme to efficiently compute the inner product of two vectors based on the inner product. In the proposed scheme, the parties can be data owners, clients or the cloud server. The three parties communicate with each other through the inner product to achieve the goal that the client can search the data in the cloud without leaking any information on the data which is stored in the cloud by an owner. Authors show the effectiveness of the proposed scheme through a security analysis and performance evaluation.

In the fifth paper, Lin et al. propose a Vehicular Crowdsourcing Localization and Tracking scheme for mounting a trajectory tracking attack in vehicular cloud computing environment. In the proposed scheme, crowdsourcing technique is applied to sample the location information of certain users. In the proposed scheme, a matrix completion technique is used to generate the proposed predictions of the users' trajectories. In order to alleviate the error disturbance of the recovered location data, Kalman filter technique is implemented and the trajectories of certain users are recovered with accuracy. Finally, authors show the effectiveness of the proposed scheme through some simulation results.

In the sixth paper, Wang et al. propose a novel auditing scheme for cloud storage services characterized by secure data transfer, provable data erasure, high error detection probability and confidential data storage. The proposed scheme can guarantee the integrity of remote data when the data are hosted on cloud servers and are transferred between two clouds, and secure deletion of the transferred data on the original cloud.

As we conclude this preface, we give special thanks to Editor-in-Chief of IJWGS Journal Dr. David Taniar for giving us the opportunity to edit the special issue. We would like to thank all authors for submitting their papers and reviewers for their good work to make it possible to publish this special issue. The support from journal manager is appreciated.