Editorial

Xiaofeng Chen*

The State Key Laboratory of Integrated Service Networks (ISN),
Xidian University,
No. 2 South Taibai Road, Yanta District,
Xi'an, Shaanxi, 710071, China
Email: xfchen@xidian.edu.cn
*Corresponding author

Jin Li

School of Computer Science and Educational Software,
Guangzhou University,
Guangzhou, 510006, China
Email: jinli71@gmail.com

Duncan S. Wong

Department of Computer Science,
City University of Hong Kong,
Tat Chee Avenue, Kowloon, 999077, Hong Kong
Email: duncanaloha@gmail.com

Biographical notes: Xiaofeng Chen received his BSc and MSc in Mathematics from Northwest University, China in 1998 and 2000, respectively. He received his PhD in Cryptography from Xidian University in 2003. Currently, he works at Xidian University as a Professor. 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 *Computing and Informatics*, *International Journal of Grid and Utility Computing*, and *International Journal of Embedded Systems*. He has served as the Program/General Chair or program committee member in over 30 international conferences.

Jin Li received his BSc in 2002 and MSc in 2004 from Southwest University and Sun Yat-sen University, both in Mathematics. He received his PhD in Information Security from Sun Yat-sen University at 2007. Currently, he works at Guangzhou University as a Professor. His research interests include applied cryptography and security in cloud computing.

Duncan S. Wong received his BEng in Electrical and Electronic Engineering with first class honours from the University of Hong Kong in 1994, MPhil in Information Engineering from the Chinese University of Hong Kong in 1998 and PhD in Computer Science from Northeastern University, Boston, MA, USA in 2002. After graduation, he was a Visiting Assistant Professor at the Chinese University of Hong Kong for one year before joining City University of Hong Kong in September 2003. He is currently an Associate Professor in the Department of Computer Science.

Cryptography is the key method and the core means to solve security and privacy issues in various real-life scenarios, especially in network transmission and personal communication. As an outstanding success, cryptography is indispensable for safeguarding security and protecting privacy in the present network environment. Nevertheless, traditional cryptographic techniques exhibit some inadequacy for the fast-developing large-scale modern networks. For example, most of the traditional cryptographic protocols have been designed only in the stand-alone execution environment and only a minority of them take 'the security of parallel execution' into consideration. Therefore, plenty of researchers put forth new cryptographic techniques so that they can provide better services to the protection of large-scale network security. This special issue on 'new cryptographic techniques for large-scale network security' attempts to highlight some of the latest research in this topic. It consists of 11 papers selected from the contributions of the 8th International Conference on Network and System Security (NSS 2014).

The paper of Li, Huang, Liu, Xu and Wu, titled 'Cooperative attribute-based access control for enterprise computing system', introduces a new access control mechanism. In the proposed system, users are divided into different groups and are affiliated with different attributes. Only members from the same group can combine their signing keys to form the signing key of a larger union set of attributes. With the union of the attributes, users can generate a signature that can be used to grant access right to the enterprise cloud system.

The paper of Shao and Yang, titled 'Proof of retrievability with efficient verification', introduces CS proof belonging to complexity theory into cloud computing, where a protocol for data integrity verification is proposed to reduce the customer's computation. Concretely, the customer's computation is poly-logarithmic only in that of the traditional protocols. The proposed protocol supports public verification even without the customer's public key and satisfies the security against semi-honest adversaries. The customer's privacy holds against both the cloud and the third-party verifier. The proposed protocol can be considered as a proper application of CS proof to integrity verification in cloud computing.

The paper of Hu, Yu, Yang, Xu, Zhou and Yuan, titled 'Weak leakage resilient extractable hash proof system and construction for weak leakage resilient CCA-secure public-key encryption', proposes generic construction of weak leakage-resilient CCA-secure key encapsulation scheme from extractable hash proofs. To this end, this paper introduces definition of weak leakage-resilient partial ABO-extractable hash proofs and proposes a method to transform extractable hash proofs to it. Then, a weak leakage resilient CCA-secure key encapsulation scheme can be derived based on it.

The paper of Chu and Feng, titled 'On the provable security of TPM2.0 cryptography APIs', defines a high-level computation model of TPM2.0 cryptography APIs and proves their security using game sequence and simulation. This paper also mentions experiments on these APIs, which show that flexibility of TPM2.0 does not reduce its performance, meanwhile, real TPM2.0 product still needs to be improved.

The paper of Jiang, Jin, Wan and He, titled 'MVP: modelling virus propagation for IPv6 wireless sensor networks, explores proper immunisation strategies and time for IPv6 WSNs under different situations, and models the virus propagation for IPv6 WSNs with anycast and multicast.

The paper of Wei, Ma, Ma and Li, titled 'A two-factor authenticated key exchange protocol based on RSA with dynamic passwords', proposes a two-factor key exchange protocol based on RSA, which can resist the e-residue attacks and replacement attacks. The user and the server only need to remember one password. The dynamic password is updated automatically in each communication session. The security of the protocol is conducted in the random oracle model under the RSA assumption.

The paper of Liu, Li, Sun, and Ajmal, titled 'Energy-efficient key agreement protocols for wireless body area networks', proposes a series of authenticated key agreement protocols based on a two-hop star network topology model, which may accommodate a number of different application situations in WBANs. The proposed protocols provide a primitive to develop efficient and secure WBAN systems.

The paper of Liu, Quan, Liu, and Zhang, titled 'Lightweight handover authentication with location privacy-preserving in mobile wireless networks', proposes an efficient handover authentication scheme by using an identity (ID)-based signcryption technique, which can considerably reduce the computation cost. The proposed scheme is also demonstrated through the security analysis to be able to realise the location privacy-preserving for mobile users and perfect forward/backward secrecy.

The paper of Zhang, Wang, Zhou, Deng, and Wang, titled 'A GAA-based batch authentication and key agreement for LTE networks', presents a batch authentication and key agreement protocol deployed in the application layer of LTE networks. In this protocol, the application server aggregates received group authentication request messages, and then delivers it to BSF for verification. User and application server can perform session agreement based on returned data after verification which will achieve end-to-end security. The designed protocol will greatly reduce the authentication delay and transmission overhead, lower the rejection probability of authentication requests and improve the quality of service.

The paper of Mandala, Ngadi, Sharif, Zahid, and Mohamed, titled 'Investigating severity of blackhole attack and its variance in wireless mobile ad hoc networks', proposes new security metrics, namely corruption routing table (CRT), compromising relay node (CRN) and compromising originating node (CON). In addition, two variants of blackhole attack, i.e., independent hybrid blackhole attack (IHBHA) and collaborative hybrid blackhole attack (CHBHA), have also been introduced for the purpose of comparative study. Through simulation in JiST/SWANS simulator, the proposed security metrics are effective to be used for measuring the severity of blackhole attack.

The paper of Luo, titled 'Anonymous hierarchical identity-based encryption without key delegation in decryption', presents a novel anonymous hierarchical identity-based encryption (AH-IBE) scheme, which is a useful combination and re-development of the existing schemes, including both hierarchical identity-based encryption (HIBE) and anonymous identity-based encryption (AIBE). The proposed scheme features the advantage that it permits direct decryption whereas former ones have to make use of key delegation mechanism. Besides, the scheme is provably secure under more favourable static assumptions and constructed in the composite-order groups. The dual system encryption technique, which is an advanced trick invented by Waters, is also successfully used.

Finally, we appreciate all authors, reviewers and editorial members for their invaluable contribution, without which this special issue cannot be reality.