Editorial

Yi Mu*

School of Information Technology and Computer Science,
University of Wollongong, Australia
E-mail: ymu@uow.edu.au
*Corresponding editor

Liqun Chen

Trusted Systems Laboratory,
Hewlett-Packard Labs,
Bristol, UK
E-mail: liqun.chen@hp.com

Xiaofeng Chen

Department of Computer Science,
Sun Yat-Sen University,
Guangzhou, China
E-mail: isschxf@mail.sysu.edu.cn

Guang Gong

Department of Electrical and Computer Engineering,
University of Waterloo,
Ontario, Canada
E-mail: ggong@calliope.uwaterloo.ca

Phi Joong Lee

Pohang University of Science and Technology, Korea
E-mail: pjl@postech.ac.kr

Atsuko Miyaji

JAIST, Japan
E-mail: miyaji@jaist.ac.jp

Josef Pieprzyk

Department of Computing,
Macquarie University,
Sydney, Australia
E-mail: josef@ics.mq.edu.au

David Pointcheval

Ecole Normale Suprieure, France
E-mail: David.Pointcheval@ens.fr

Tsuyoshi Takagi

School of Systems Science Information,
Future University, Hakodate, Japan
E-mail: takagi@fun.ac.jp

Jacques Traore

Network and Service Security Division,
France Telecom R&D, France
E-mail: jacques.traore@francetelecom.com

Jennifer Seberry and Willy Susilo

School of Information Technology and Computer Science,
University of Wollongong, Australia
E-mail: jennie@uow.edu.au
E-mail: wsusilo@uow.edu.au

Huaxiong Wang

Macquarie University, Australia
E-mail: hwang@ics.mq.edu.au

Fangguo Zhang

School of Information Science and Technlogy,
Sun Yat-Sen University, China
E-mail: isdzhfg@zsu.edu.cn

Biographical notes: Yi Mu is an Associate Professor of School of Information Technology and Computer Science, University of Wollongong, Australia. He received his PhD from the Australian National University in 1994. His current research interests include network security, electronic commerce security, wireless security, access control, computer security and cryptography. He has served in program committees of a number of international conferences and editorial boards of five international journals. He is a senior member of the IEEE and a member of the IACR.

Liqun Chen is a Research Scientist in the Trusted Systems Laboratory of Hewlett-Packard Laboratories in Bristol, which she joined in 1997. Her research interests are in trusted computing, information security and cryptography. She served as an Editor of two ISO/IEC security technique standards (ISO/IEC 10118-3 and ISO/IEC 11770-4) and she is presently serving as a co-editor of ISO/IEC 14888-3).

Xiaofeng Chen is an Associate Professor in the Department of Computer Science at Sun Yan-Sen University, Guangzhou, China. He received his PhD in Cryptography from School of Communication Engineering, Xidian University in 2003. His main research interests include public key cryptography and E-commerce security.

Guang Gong (BS 1981, MS 1985, PhD 1990) is a Professor in the Department of Electrical and Computer Engineering at University of Waterloo, Ontario, Canada. Her research interests are in the areas of sequence design, cryptography and network security and she is an Associate Editor for Sequences for IEEE Transactions on Information Theory.

Phi Joong Lee received his BS and MS from Seoul National University and his Engineer degree and PhD from U.C.L.A. Before joining Pohang University of Science and Technology (POSTECH) in Korea, he worked for Jet Propulsion Laboratories in Pasadena, CA from 1980 to 1985 and for Bell Communications Research (Bellcore) in Morristown, NJ from 1985 to 1990. He was the Dean of Graduate School for Information Technology, POSTECH and the Director of POSTECH Information Research Lab from 2000 to 2003 and also served as the President of Korea Institute of Information Security and Cryptology in 2004, His current interest includes all aspects of information security and cryptology.

Atsuko Miyaji received the Dr. Sci. degrees in Mathematics from Osaka University, Osaka, Japan in 1997. She had joined Matsushita Electric Industrial Co., LTD until 1998. She has been an Associate Professor at JAIST (Japan Advanced Institute of Science and Technology) since 1998. She has joined the Computer Science Department of University of California, Davis since 2002. She is a member of the International Association for Cryptologic Research, the Institute of Electronics, Information and Communication Engineers, the Information Processing Society of Japan and the Mathematical Society of Japan.

Josef Pieprzyk is a Professor in the Department of Computing, Macquarie University, Sydney, Australia. He is the Director of Centre for Advanced Computing – Algorithms and Cryptography. His research interest includes cryptography, computer network security, database security, design and analysis of cryptographic algorithms, algebraic analysis of block and stream ciphers, theory of cryptographic protocols, secret sharing schemes, threshold cryptography, copyright protection, e-Commerce and web security.

David Pointcheval is a CNRS Researcher. He received his PhD in cryptography at the Ecole Normale Supérieure, Paris, France and is now the head of the Crypto Team at ENS. His main research topic is the 'provable security' of protocols and primitives. He is the author of hundreds of international publications and the inventor of nine patents.

Tsuyoshi Takagi had engaged in the research on network security at NTT Laboratories from 1995 to 2001. He was an Assistant Professor in the Department of Computer Science at Technische Universität Darmstadt until 2005. He is currently an Associate Professor in the School of Systems Science Information at Future University-Hakodate, Japan.

Jacques Traore is a Senior Security Engineer in the Network and Service Security Division at France Telecom R&D. He received a PhD in Applied Mathematics from the University of Caen. His current research interests include network security, cryptography and privacy protection. He has been recently involved in several research projects, on national and European levels, related to electronic voting.

Jennifer Seberry is a Professor of School of Information Technology and Computer Science at University of Wollongong, Australia. She received a PhD in Computational Mathematics in 1971. She has successfully supervised 27 PhD candidates and has published more than 350 scholarly books and papers.

Willy Susilo is an Associate Professor at the School of Information Technology and Computer Science at the University of Wollongong. His research interest is in the area of digital signatures and cryptography in general. His contributions include the design of short signature schemes and variants of signature schemes.

Huaxiong Wang received a PhD in Mathematics from the University of Haifa, Israel (1996) and a PhD in Computer Science from the University of Wollongong, Australia (2001). His research interests include cryptography, information security, coding theory, combinatorics and theoretical computer science. He is on the editorial boards of Designs, Codes and Cryptography, *Journal of Communications* and *Journal of Communications and Networks* and was the Program Co-Chairs of ACISP04 and CANS05.

Fangguo Zhang received a PhD in Cryptography from Xidian University, Shannxi, China in 2001. He is presently a Professor of School of Information Science and Technology, Sun Yat-Sen University, China. His research interests are Pairings Based Cryptosystems, Elliptic Curve and Hyperelliptic Curve Cryptography and Provable Security.

Cryptography plays a key role in network security. Advances of cryptography can make computer networks more secure. Computer technologies have been pushing forward computer networks for high speed and broad bandwidth. Therefore, new cryptographic methods and tools must follow up in order to adapt to these new technologies. Recent attacks on computer networks, especially on IEEE 802.11 and IEEE 802.15, are increasing, since underlying radio communication medium for wireless network provides serious exposure to attacks against wireless networks. Security must be enforced to suit the emerging technologies. This Special Issue aims to provide a platform for security researchers to present their newly developed cryptographic technologies in network security. Areas of interest for this special journal issue include, but are not limited to, the following topics: ad hoc network security, anonymity in networks, authentication in network and wireless systems, cryptographic algorithms and their applications to network security, cryptanalysis of network security schemes, encryption in network and wireless systems, e-mail security, data integrity, fast cryptographic algorithms and their applications, identity-based cryptography in network and mobile applications, IP security, key management, multicast security, mobile and wireless system security, privacy protection, security group communications, security in internet and WWW, security in Peer-to-Peer networks, secure routing protocols and security in sensor networks.

We received 53 manuscripts. Ten manuscripts were selected for this Special Issue. The reviewing process took three months. Each manuscript was blindly reviewed by normally three (some of them two or four) reviewers consisting of guest editors and external reviewers.

The first paper in this Special Issue is Efficient multicast stream authentication for the fully adversarial network model, by Christophe Tartary and Huaxiong Wang. This work addresses stream authentication issues of multicast. It describes a coding approach for multicast stream authentication using the list-decoding property of Reed-Solomon codes, while assuming that an adversary has the ability to drop, reorder or inject data in the network. The result shows a significant improvement over the previously proposed scheme due to Lysyanskaya et al.

The second paper in this Special Issue is Aggregate designated verifier signatures and application to secure routing, by Raghav Bhaskar, Javier Herranz and Fabien Laguillaumie. This work describes a novel designated verifier signature scheme and introduces the notion of aggregate designated verifier signature, following the notion of aggregate signature introduced by Boneh et al. The resulting schemes are proved to be secure under the CDH assumption, in the random oracle model. It also explains the possible application of aggregate designated verifier signatures to the authentication of messages in routing protocols.

The third paper in this Special Issue is LIP: a lightweight inter-layer protocol for preventing packet injection attacks in mobile ad-hoc network, by Hung-Yuan Hsu, Sencun Zhu and Ali R. Hurson. This work proposes a lightweight inter-layer protocol for preventing packet injections based on an efficient local broadcast authentication mechanism. Through detailed simulation study, it shows that LIP is scalable and it incurs small bandwidth overhead as well as little impact on the traffic delivery ratio even in the case of high node mobility.

The fourth paper in this Special Issue is On the design of secure protocols for hierarchical sensor networks, by Leonardo B. Oliveira, Hao Chi Wong, Antonio A.F. Loureiro and Ricardo Dahab. This work proposes some secure protocols for securing heterogeneous hierarchical WSNs with an arbitrary number of levels and symmetric key schemes.

The fifth paper in this special issue is Server side hashing core exceeding 3 Gbps of throughput, by Harris E. Michail, George A. Panagiotakopoulos, Vasilis N. Thanasoulis, Athanasios P. Kakarountas and Costas E. Goutis. This work presents a new technology for increasing frequency and throughput of the currently most used hash function which is SHA-1. This technique involves the application of spatial and temporal precomputation. Comparing to conventional pipelined implementations of hash functions the proposed technique leads to an implementation with more than 75%.

The sixth paper in this Special Issue is Preventing or utilising key escrow in identity-based schemes employed in mobile ad hoc networks, by Katrin Hoeper and Guang Gong. This work focuses on the role of the Key Generation Center (KGC) as a key escrow, a property that is inherent to all identity-based cryptography schemes and discusses the two faces of key escrow in MANETs, where our analytical results show that in many MANET applications the KGC can be prevented from being a key escrow. On the other hand, the results of this paper illustrate how a KGC can utilise spy nodes to monitor nodes in a MANET, as needed in some applications.

The seventh paper in this special issue is On security proof of McCullagh–Barreto's key agreement protocol and its variants, by Zhaohui Cheng and Liqun Chen. The work revisits these three security proofs of an identity-based authenticated key agreement protocol due to McCullagh and Barreto and Xie and shows that all the reductions in these proofs are invalid. It provides a modification of one of the schemes and provides a security analysis in the Bellare-Rogaway key agreement model.

The eighth paper in this special issue is Cryptanalysis of an elliptic curve cryptosystem for wireless sensor networks, by Kevin M. Finnigin, Barry E. Mullins, Richard A. Raines and Henry B. Potoczny. This work presents a brute-force attack on an elliptic curve cryptosystem implemented on UC Berkley's TinyOS operating system for wireless sensor networks. The attack exploits the short period of the Pseudorandom Number Generator (PRNG) used by the cryptosystem to generate private keys.

The ninth paper in this Special Issue is Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks, by Dijiang Huang. This work presents pairing-based encryption/decryption, key exchange, blind certificate and revocation solutions for anonymous communications. The proposed approach provides the following some novel properties compared to traditional approaches.

The tenth paper in this Special Issue is Strong password-based authentication in TLS using the three-party group Diffie–Hellman protocol, by Michel Abdalla, Emmanuel Bresson, Olivier Chevassut, Bodo Möller and David Pointcheval. This work shows that the three-party group Diffie–Hellman key exchange can help protect against phishing attacks. They proposed password-based ciphersuites for the Transport Layer Security (TLS) protocol that are not only provably secure but also believed to be free from patent and licensing restrictions based on an analysis of relevant patents in the area.

Finally, we would like to thank all authors who have submitted their manuscripts to this Special Issue and the following external reviewers for their invaluable contributions to the reviewing process: Yamada Asahiko, Gildas Avoine, Sebastien Canard, Olivier Chevassut, Hervé Debar, Henri Gilbert, Marc Girault, Kishan Gupta, Yassir Nawaz, Katrin Hoeper, Xinyi Huang, Yong Ho Hwang, Takeru Ishihara, Shaoquan Jiang, Jin Ho Kim, Tae Hyun Kim, Steve Kremer, Noboru Kunihiro, Eun Jeong Kwon, Jin Li, Xinbin Lin, Shin'ichiro Matsuo, Lan Nguyen, Masayuki Numao, Jung Hyung Park, Eun-Kyung Ryu, Jae Woo Seo, SeongHan Shin, Herve Sibert, Hung-Min Sun, Yuko Tamura, Shidi Xu, Guomin Yang, Yeon Hyeong Yang and Dae Hyun Yum. We would like to thank the Editor-in-Chief, Professor Yang Xiao, for giving us this great opportunity of organising this Special Issue.