Editorial

Arcangelo Castiglione*

Department of Computer Science,
University of Salerno,
Fisciano 84084, Italy
Email: arcastiglione@unisa.it
*Corresponding author

Jin Li

Department of Computer Science,
Guangzhou University,
Guangzhou 510006, China
Email: jinli71@gmail.com

Zhe Liu

Institute for Quantum Computing,
University of Waterloo,
200 University Avenue West Waterloo, Ontario, N2L 3G1, Canada
Email: zhelu.liu@uwaterloo.ca

Marek R. Ogiela

Cryptography and Cognitive Informatics Research Group,
AGH University of Science and Technology,
Krakow 30-059, Poland
Email: mogiela@agh.edu.pl

Biographical notes: Arcangelo Castiglione received his BS, MS and PhD in Computer Science from the University of Salerno, Italy. In 2015, he was a Visiting Researcher at the Laboratory of Cryptography and Cognitive Informatics, AGH University of Science and Technology, Krakow, Poland, and School of Mathematics and Computer Science, Fujian Normal University, China. He is currently a Postdoctoral Fellow at the Department of Computer Science and Adjunct Professor at the Department of Industrial Engineering, University of Salerno, Italy. His research mainly focuses on cryptography, multimedia data protection and network security. He is an Associate Editor for several journals, and has been a guest editor for several special issues and volume editor for *Lecture Notes in Computer Science* (Springer). He is a member of various program committees for international conferences and reviewer for several scientific journals and conferences.

Jin Li received his BS in Mathematics from the Southwest University, Chongqing, China in 2002, MS in Mathematics and PhD in Information Security from the Sun Yat-sen University, Guangzhou, China in 2004 and 2007, respectively. He served as a Senior Research Associate for the Korea Advanced Institute of Technology, Daejeon, South Korea, and Illinois Institute of Technology, Chicago, IL, USA, from 2008 to 2010. He is currently a Professor at the Guangzhou University, Guangzhou, China. He has authored over 40 papers in international conferences and journals. His research interests include design of secure protocols in cloud computing (secure cloud storage, encrypted keyword search, and outsourcing computation) and cryptographic protocols.

Zhe Liu is a Full Professor in the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics. He is also a Research Fellow at the SnT, University of Luxembourg. He received his PhD from the Applied Cryptography Group, University of Luxembourg in 2015 and the prestigious FNR Outstanding PhD Thesis Award in 2016. His research areas include computer arithmetic and cryptographic engineering for pre-quantum and post-quantum cryptography.

Marek R. Ogiela is a Professor of Computer Science, cognitive scientist and cryptographer, and Head of Cryptography and Cognitive Informatics Laboratory in Krakow, Poland. He is a member of numerous world scientific associations, including SPIE Fellow member, IEEE Senior member, and at the Interdisciplinary Scientific Committee of the Polish Academy of Arts and Sciences. He is the author of more than 400 scientific international publications on pattern recognition and image understanding, artificial intelligence, cybernetics, cryptography and information theory.

Security and privacy in complex large-scale computing systems for big data management is expected to be one of the hottest topics in the next few years. Indeed, both academia and industry widely recognise the inherent potential of such systems. For organisations employing big data, the boundaries between the use of private clouds, public clouds, virtualisation technologies, internet of things (IoT), etc. are sometimes very thin. Furthermore, our society is constantly influenced by different lifestyle shifts, driven by recent technological advances beyond the more established trend of cloud computing, e.g., cyber-physical systems (CPS), cyber-physical social lifestyles augmented by social media, smart clothing, nano-sensors, flexible electronics, etc. Therefore, assessing the security and privacy of such systems is today a main concern for computer scientists, engineers and practitioners.

Although research on finding approaches to solve real-world security and privacy problems has been conducted in the public domain for decades, and well-established paradigms and techniques have been proposed to solve several security problems in our lives, today new challenges emerge due to the additional features beyond the basic security requirements, arising from real-world constraints, changing needs or socio-technological revolutions.

The aim of this special issue was to seek recommendations and innovative methods which can be successfully delivered to multi-disciplines, providing quality papers focused on security and privacy in complex large-scale computing systems, whose lessons learned will be transferable across disciplines to encourage interdisciplinary research and funding activities essential for progressive research and development. More in general, we welcomed all things non-conventional, i.e., tools, techniques and frameworks influenced by recent and/or future socio-technological revolutions.

This special issue carries revised and substantially extended versions of selected papers presented at the 12th International Conference on Green, Pervasive and Cloud Computing (GPC 2017), as well as it carries original articles related to the call of this conference.

Among the 20 submissions, just seven have been accepted for publication. The evaluation process of the submissions has been made in a rigorous way, by professionals coming from several sectors, including both academia and industry.

The first contribution, co-authored by Wang et al. is ‘A high efficient map-matching algorithm for the GPS data processing intended for the highways’. The article proposes a highly efficient map-matching algorithm intended for the analysis of big data collected at the highway, based on the topological characteristics of the highway road network. The algorithm presented in this paper has two main improvements: it uses a fuzzy estimation algorithm to reduce the redundant calculations in map-matching processing on the arterial links, as well as it introduces a new parameter to evaluate the most suitable travelling path for vehicles on the highway road network. Experimental results show that the proposed algorithm improves the efficiency and ensures, at the same time, the high accuracy of the highway GPS data processing.

Error reconciliation is an important technique for learning with error (LWE) and ring-learning with error (RLWE)-based constructions. In the article ‘Comparison analysis and efficient implementation of reconciliation-based RLWE key exchange protocol’, co-authored by Gao et al., the authors propose a comparative analysis of two error reconciliation-based RLWE key exchange protocols: Ding et al. in 2012 (DING12) and Bos et al. in 2015 (BCNS15). The authors take such protocols as examples to explain the core idea of error reconciliation, besides building key exchange based on the RLWE problem. Again, the authors implement such protocols to assess real-world performance and compare them comprehensively. Finally, the authors analyse the LWE key exchange Frodo, which uses an improved error reconciliation mechanism in BCNS15.

Owing to the diffusion of the internet, the number of social network individuals increases and network data are poised for a massive change in trends. In the article ‘Distributed and personalised social network privacy protection’, co-authored by Zhang et al., the authors propose a personalised k-degree-m-label (PKDML) anonymity model. More precisely, the authors design and implement a distributed and personalised k-degree-m-label (DPKDML) anonymisation algorithm, which exploits the ‘vertex-centric’ GraphX programming model. Experimental results validate the authors’ proposal.

In the article ‘A delegation token-based method to authenticate the third party in TLS’, co-authored by Yan et al., the authors propose a delegation token-based

method to authenticate the proxy server, with multi-level proxy servers being taken into consideration. Again, to improve the proposed method in terms of time consumption, the authors use a client-based cache strategy. The security of the proposed method has been analysed and experimental results demonstrate the effectiveness of authors' proposal.

In order to improve the multi-user data sharing mechanism in hybrid clouds and enhance the security of hybrid clouds, in the article 'A secure storage scheme with key-updating in hybrid cloud', co-authored by Gao et al., the authors propose a new security storage model for hybrid clouds, which combines the public cloud cost savings and elasticity with the private cloud security and customisation. In addition, by exploring the security of data storage and interoperability of hybrid clouds, this paper proposes a forward-secure key-updating encryption scheme, which ensures the privacy of data in hybrid clouds.

Intrusion detection systems (IDS) have become a popular cloud security technology to detect attacks in a wide variety of networks. Cloud IDS is a better solution to achieve a higher level of security, while maintaining its individuality. The cloud IDS is the most widely used technique when the system consists of IDS connected over the network, in combination with various anomaly detection techniques. In the article 'Survey of intrusion detection techniques and architectures in cloud computing', co-authored by Sharma et al., the authors provide an extensive survey of various cloud-based IDS, implemented in a cloud environment for dealing with several security issues. This paper also discusses architectures of various cloud IDS.

In the last article, 'ROI-based fragile watermarking for medical image tamper detection', co-authored by Goléa and Melkemi, the authors propose a region of interest (ROI)-based fragile watermarking scheme for medical image tamper detection. The proposed methodology is inspired by network transmission, where the transmitted message is divided into packets of fixed size and redundant information is added to each packet to deal with errors. Depending on the degree of alteration and interest in the packet, the receiver can ask the sender to retransmit only the corrupted packets. Experimental results carried out on six different modalities of medical images show the validity of the proposed approach in terms of imperceptibility and efficiency.

Editing this special issue has been a very demanding and stimulating experience, since we dealt with several good contributions. To this aim, we would like to warmly thank all the authors for their outstanding researches. Each of the accepted articles has been subject to a rigorous peer review procedure and has been assessed by several independent reviewers. Moreover, a special thank you goes to the anonymous reviewers, who provided constructive feedback to the authors to improve their works. Last but not least, we are grateful to the editorial board of this special issue and to Prof. Kuan-Ching, Editor-in-Chief of the *International Journal of High Performance Computing and Networking*, for his great support throughout the entire publication process.