Editorial

Fatos Xhafa*

Department of Computer Science,
Technical University of Catalonia,
Campus Nord, Ed. Omega,
C/Jordi Girona 1-3, 08034 Barcelona, Spain
Email: fatos@cs.upc.edu
*Corresponding author

Xu An Wang

Key Laboratory of Cryptography and Information Security,
Engineering University of Chinese Armed Police Force,
Wujing Road No. 1, Sanqiao Town, Xi'an City,
Shaanxi Province, 710086, Xi'an, China
Email: wangxazjd@163.com

Biographical notes: Fatos Xhafa received his PhD in Computer Science from the Technical University of Catalonia (UPC), Barcelona, Spain, where he holds the permanent position of a Professor Titular d'Universitat. He was a Visiting Professor at the University of London, UK (2009/2010) and Research Associate at the Drexel University, Philadelphia, USA (2004/2005). He has widely published in peer reviewed international journals, conferences/workshops, book chapters and edited books and proceedings in the field. He is the Editor-in-Chief of the *International Journal of Space-based and Situated Computing*, and *International Journal of Grid and Utility Computing*, Inderscience. He is actively participating in the organisation of several international conferences. His research interests include parallel and distributed algorithms, combinatorial optimisation, networking, cloud, grid and P2P computing.

Xu An Wang received his BS and MS in Computer Science and Cryptography from Engineering University of Chinese Armed Police Force, and received his PhD in Cryptography from Xidian University. He is currently an Associate Professor in the Engineering University of Chinese Armed Police Force. His research interests are public key cryptography, cloud security, provable security and information security. He has published more than 60 research papers at referred national and international journals, conference proceedings. He has served as the Program Co-chair or program committee member in several international conferences.

Along with the rapid development of cloud computing and big data technology, more and more individuals, businesses, companies, institutions and organisations, etc. prefer to upload their datasets to the cloud for convenient management and maintenance. However, security issues arise and are needed to be addressed before these paradigms can be adapted widely. Trusted computing can play an important role to establish a trusted relationship among different parties in cyber-space. Information hiding is also an important branch of modern information security, which mainly focuses on transferring some secret information via open media, such as texts, pictures, videos, etc. in some unnoticeable way.

This special issue on 'Advances in intelligent methods for trusted computing and information hiding' aims to bring together some new advanced intelligent techniques on these aspects. It comprises eight papers carefully selected from the contributions of the 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC 2015) and other excellent submissions directly to this special issue. They are the following:

In Kong et al.'s paper titled as 'Improved phrase search construction over encrypted data in cloud storage', the authors present a security analysis of Kissel's scheme and show that the cloud service provider can obtain some new phrases trapdoors and search outcomes based on the clients' phrase query. They also propose an improvement to simplify Kissel's scheme and enhance its security. The comparison results show their scheme is more secure and efficient.

In Cao et al.'s paper titled as 'Selective maintenance for maximising system availability: a simulation approach', a simulation method is proposed to optimally select the maintenance schemes, including the selected components to be repaired and maintenance tasks allocation with the objective of maximising system availability. Genetic algorithm (GA) is adopted to optimally allocate maintenance tasks to the limited repairman. An illustrative example is presented to demonstrate the applicability. Furthermore, the

effects of repairman and mission duration on system availability are discussed in the paper.

In Jin et al.'s paper titled as 'A new socio-rational secret sharing scheme', the authors introduce the concept of a socio-rational secret sharing scheme, in which shares are delivered based on players reputation and the way they contact with other participants. At the secret sharing stage, weights of players are defined such that participants who cooperate will get more shares than those who defect. Their intention is that, in real world applications, participants of a secure scheme may have different levels of importance (i.e., the weight of shares a player owns) as well as reputation (i.e., cooperation with other players for the share renewal or secret recovery). In their proposed schemes, both the traditional and rational players are considered and analysed in an unconditionally secure setting.

In Zeng et al.'s paper titled as 'Detecting blurred image splicing using blur type inconsistency', the authors propose a novel framework for image splicing detection based on partial blur type inconsistency. In this framework, after the cepstrum-based image transforming, a blur type classification parameter is extracted from the spectrum characteristics of spliced blurred image. The blurred image is restored based on the blur kernel which is constructed by estimating the blur parameters. Finally, a fine measure method is applied to segmentation inconsistent region in restored images that contain large amounts of ringing effect. Simulation results show the proposed method is very effective.

In Lei et al.'s paper titled as 'Intrusion detection techniques based on improved intuitionistic fuzzy neural networks', three novel intrusion detection techniques have been proposed. The first technique combines the theories of both intuitionistic fuzzy sets (IFS) and artificial neural networks (ANN) together, which lead to much fewer iteration numbers, higher detection rates and sufficient stability. The second technique is based on non-subsampled shearlet transform (NSST) domain ANNs, including employing multi-scale geometry analysis (MGA) of NSST and the train characteristics of ANN together. Lastly, an efficient anomaly analysis method that is proved to be more efficient and less complex than the existing techniques has been proposed. The approach relies on monitoring the security state by using a set of accurate metrics. The NSST is used to decompose these metrics. Attacks are viewed as singularities that arise in some specific points of time. Experimental results indicate that these three proposed techniques are all effective and promising.

In Sun et al.'s paper titled as 'An information hiding method based on context-based adaptive variable length coding', a real-time video information hiding method in CAVLC for H.264/AVC is proposed, which combines information hiding with CAVLC process, and embeds the secret information in the number of trailing coefficients of in the number of trailing coefficients of 4 × 4 macroblocks. Experimental results show that the embedding process cannot bring detectable video degradation, and only cause a small change in the length of the video stream. Moreover, the embedded secret information can be recovered correctly when being transferred under different RTP lost channels. And the secret information can be extracted directly from the encoded stream without resorting to the original video.

In Zhou et al.'s paper titled as 'Properties of two-layer FHE and their applications', the authors extend three useful processes of the AP14 (an famous two-layer FHE): HTG, FDDec and negative, which are essential to many applications. HTG can transform a HEPerm ciphertext, a ciphertext of permutation matrix in AP14, to a small GSW ciphertext. FDDec can decrypt a HEPerm ciphertext directly. Secondly, they concluded the rules of application about their scheme and constructed an efficient bits comparator as an example of application. At last, they find a solution based on the equality test for the problem of password leakage, which can protect the password and preserve the bypass function, when the database of password was compromised.

In the last paper titled as 'On the influencing mechanism of unsafe behaviour of coal miners based on hierarchical regression', Li and Di explore the impact of job stress on the unsafe behaviour of coal miners, and also explore mediating effect of job burnout on the relationship between the job stress and unsafe behaviour of coal miners. A total of 194 valid samples were collected and analysed to draw following conclusions: job stress and unsafe behaviour of coal miners have a significantly positive correlation; job stress has mediating effect on the relationship between the job stress and unsafe behaviour of coal miners.

Acknowledgements

The guest editors would like to thank Prof. Nadia Nedjah (Editor-in-Chief of *IJICA*) for providing us the opportunity to edit this special issue. We would like to thank Ms. Liz Harris, Inderscience Journal Manager for the publishing work for this special issue. Finally, we thank all authors, reviewers and editorial members for their supporting for this special issue.