GUEST EDITORIAL PREFACE

Special Issue on Advanced Algorithms for Efficient, Reliable and Secure Information Systems

Fatos Xhafa, Universitat Politècnica de Catalunya, Barcelona, Spain

Xu An Wang, Engineering University of CAPF, Xi'an, China

The growth of importance, usage, complexity of information systems has brought new challenges to its reliability and security. Not only the security protocols and schemes are important but the fault-tolerant hardware is having a more and more important role, especially with the cloud and big data information systems. Building security and reliable systems requires not only efficient security algorithms but also advanced fault tolerant and detect techniques. Indeed, for complex information systems, it is a real challenge to implement an efficient code that respects the security specification but also provides other extra-functional properties like scalability and fault tolerance. The cooperation design of software and hardware is an increasing trend in the construction of reliable and secure information systems. This special issue brings together research articles covering diverse hardware and software techniques for efficient, reliable and secure information systems, including fault diagnosis method, method for improving data security in register files, maximum lyapunov exponent, reliable face detection, high-capacity covering code, optimized multilinear maps and homomorphic encryption over large message space.

The papers in this special issue are arranged as follows.

Wu *et al*. in the first paper "Research on fault diagnosis method using improved multi-class classification algorithm and relevance vector machine" proposed a fault diagnosis method based on improved multi-class classification algorithm and relevance vector machine (RVM). Numerical simulations and experiments results both demonstrate that the proposed method performs significantly better than other traditional methods in terms of increasing the diagnostic accuracy, optimizing the voting results, strengthening the diagnostic confidence and identifying the hidden classes.

In the second paper "Method for improving data security in register files based on multiple pipeline restart" proposed by Chen *et al*., the author discusses on the fault-tolerant technique

targeting for register files. Based on data replica and pipeline restart, the method of improving the data security and reliability in register files is presented. The proposed method is evaluated and the results show that the hardware overhead increases by only 2%, whereas the reliability of data in register file increases by more than 2.5 times. This method can significantly improve the data security in the register file without distinct overhead increasing.

In the third paper "A Study on components and features in face detection", Yang et al. propose the method of components and feature extraction in face detection. In their paper, face is looked on as a whole composed of several parts from up to down. Each region is identified by a local classifier and is assigned a preliminary part label. Experiment results show that the methods can improve the detection rate and enhance the robustness of face detection in case of occlusion.

Tian *et al*. in the fourth paper "A high-capacity covering code for voice-over-IP steganography" proposed a (2n−1, 2n) covering code, which can hide 2n−1 bits of secret messages into 2n bits of cover messages with not more than n-bit changed. The experimental results show that our scheme can provide good performance on both steganographic transparency and embedding capacity, and achieve better balance between the two objectives than the existing ones.

In the fifth paper "An Improved Multilinear map and its applications" proposed by Gu is discussed on a new construction of multilinear map using random matrix, which supports the applications for public tools of encoding in the GGH13 map. His construction removes the special structure of the ring element in the principal ideal lattice problem, and avoids potential attacks generated by algorithm of solving short principal ideal lattice generator.

Finally, Chen *et al*. in the final paper "An Additively homomorphic encryption over large message space", proposes an additively homomorphic encryption scheme based heavily on smart-vercauteren encryption scheme, where both schemes each work with two ideals I and J. As a contribution of independent interest, a two element representation of the ideal I is given and proven by factoring prime numbers in a number field. The results indicate that this construction has much larger message space than SV10 scheme.

We would like to thank all the authors for their valuable contributions and the reviewers for their time and constructive feedback during several rounds of review and revision. We would like to sincerely thank Prof. Ghazi Alkhatib, Founder & Editor-in-Chief of IJITWE journal, for the opportunity to edit this special issue and for his encouragement. The support by the Journal's Editorial team at IGI is highly appreciated.

Fatos Xhafa's work has been partially supported by Research Project of the Spanish Ministry for Economy and Competitiveness (MINECO) and the European Union (FEDER funds) under grant COMMAS (ref. TIN201346181C21R).

Fatos Xhafa
Xu An Wang
Guest Editors
IJITWE