Editorial: *IEEE Transactions on Sustainable Computing*, Special Issue on Cryptography and Data Security in Sustainable Computing (Part 2)

Karl Andersson, Xiaofeng Chen, Christian Esposito, and Eric Rondeau

THE accepted papers in this special issue focus on cryptography and data security in sustainable computing. With the proliferation of several kinds of attacks towards ICT infrastructures and the relative effects caused by a successful compromise of them, data security is of pivotal importance in our current society. As a practical example, health-related data is rapidly being digitalized passing from paper-based communications among patients and physicians to computer-based ones. However, the occurrence of data leakage is increasing, with the consequence of stealing sensitive personal information from the leaked health-related data. In order to protect the ICT infrastructures from these attacks, several solutions have been proposed, where cryptography plays a key role. Despite being able to provide a suitable degree of security and privacy, such solutions have not been designed by taking care of their energy consumption and resource usage. Therefore, they are not optimal in the case of resource-constrained systems, such as sensor networks, and are under radical rethinking in order to be effectively adopted in such context. Moreover, the recent increasing attention to climate changes and environmental issues are leading a considerable debate on how changing the current computing technologies so as to have less severe effects on the global warming and resource usage. Such a debate involves also the current cryptosystems and the other widely-accepted solutions to provide data security, so as to modify them by considering their sustainability. Thus, this special issue aims at collecting updated outstanding papers that illustrate the latest achievements and development updates concerning cryptography and data security solutions, issues, applications, trends, and implementations in sustainable computing.

This special issue section consists of six of the 12 accepted papers and focuses on a trust inference framework in MANETs, data security in health care remote locations, encryption using information fusion techniques, a key exchange protocol for roaming, privacy enhanced location sharing, and 3D polarized beamforming in power domain NOMA Systems:

1. TSUSC-2017-07-0063: A Novel Light-Weight Subjective Trust Inference Framework in MANETs,
2. TSUSC-2017-08-0067: A Sustainable Solution to Support Data Security in High Bandwidth Health Care Remote Locations by Using TCP CUBIC Mechanism,
3. TSUSC-2017-09-0101: An Encryption Approach Using Information Fusion Techniques Involving Prime Numbers and Face Biometrics,
4. TSUSC-2017-09-0086: A Mobile Intelligent Terminal Based Anonymous Authenticated Key Exchange Protocol for Roaming Service in Global Mobility Networks,
5. TSUSC-2017-07-0061: Privacy Enhanced Location Sharing for Mobile Online Social Networks, and
6. TSUSC-2017-09-0085: Inter-Beam Interference Cancellation and Physical Layer Security Constraints by 3D Polarized Beamforming in Power Domain NOMA Systems.

Karl Andersson
Xiaofeng Chen
Christian Esposito
Eric Rondeau
Guest Editors

- *K. Andersson is with the Lulea University of Technology, 971 87, Luleå, Sweden.*
- *X. Chen is with Xidian University, Xi'an, Shaanxi, China.*
- *C. Esposito is with the University of Napoli "Federico II", Napoli, NA 80138, Italy.*
- *E. Rondeau is with the Université de Lorraine, CRAN CNRS, CRAN UMR 7039, Nancy, France.*

Digital Object Identifier no. 10.1109/TSUSC.2019.2912235

2377-3782 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.