



Security and Communication Networks
By Wiley InterScience
<http://www.interscience.wiley.com/security>
(Online ISSN: 1939-0122, Print ISSN: 1939-0114)

“Special Issue on Security Technologies and applications for Convergence environments”

Recently, convergence environments have gained much attention in the community. The research on converged technologies and applications covers the topics of seamless, secure, and intuitive access for distributed processing of various computing technologies and applications. Due to the wide proliferation of wireless technologies, the fast processing speed is of ultimate importance. There has been much research effort made in the literature to provide the communications and computing through distributed and parallel processing over the scattered networks. More specifically, the convergence environments represent an interdisciplinary field with its roots in economics, mathematics and engineering, involving the technologies and applications in the next generation environments including ubiquitous, pervasive, smart grid, P2P computing, etc. In addition, the reliable security solutions that rely on advanced cryptography are required to ensure confidentiality, integrity, and availability for secure and convenient life in the convergence environments. This special issue provides an international forum for presentation and showcase of the most recent advances on various aspects of cryptography, security, and technologies and applications for convergence environments. It will reflect the state-of-the-art of the computational methods, involving theory, algorithm, numerical simulation, error and uncertainty analysis and/or application of innovative processing techniques in engineering, science, and other disciplines related to the convergence security (CS).

The submissions are expected to focus on novel approaches for the CS and to present high quality research works for tackling the problems arising from the fast-growing CS research. This special issue will serve as a source for education, information, and reference to students, professionals, and researchers interested in CS technologies and applications.

Topics of interest include (but are not limited to)

- Cryptography and Security Protocol for CS
 - Public Key Cryptosystems for CS
 - Design and Analysis of Cryptographic Algorithms for CS
 - Pairing Based Cryptography for CS
 - Authorization and Access Control for CS
 - Identity and Trust Management for CS
 - Digital Rights management for CS
 - Computer Forensics for CS
 - Trust computing for CS
- Security Applications and Services for CS
 - Smartphone Security issues
 - Security for Open convergence system
 - Security for M2M Platform
 - Security and privacy for intelligent vehicular systems
 - Security for Broadband convergence Network (BcN).
 - IPTV security services in the BcN

Guests Editors

Prof. Jong Hyuk Park
Corresponding Guest Editor
Seoul National University of Technology, Korea
Email: parkjonghyuk1@hotmail.com

Prof. Shih-Jeng Wang,
Central Police University, Taiwan
Email: dopwang@gmail.com

Dr. Damien Sauveron
XLIM - UMR CNRS 6172, Université de
Limoges, France
Email: Damien.Sauveron@unilim.fr

Important Dates

Manuscript submission deadline: July 1, 2010
Notification of acceptance: Dec. 1, 2010
Final Manuscript Due: Dec. 31, 2010
Publication of special issue: 2nd or 3rd Quarter, 2011 (Tentative)

Submission Details

Original and high quality contributions that are not yet published or that are not currently under review by other journals or conferences are sought. For manuscript submission, authors should follow the guidelines described in the <http://www.interscience.wiley.com/security>. Prospective authors should submit their paper(s) online at <http://mc.manuscriptcentral.com/scn>. When submitting the papers, the authors should choose the “Manuscript Type” as “Special Issue”, enter the “Running Head” as “SCN-SI-024” and the “Special Issue Title” as “Advanced Security Technologies and applications for Convergence environments”, respectively. Contributing authors might also be asked to review some of the papers submitted to this special issue.