

Theme Issue – Call for Papers

Personal and Ubiquitous Computing
ISSN : 1617-4909

1. Title of Theme Issue

Advanced security technologies and applications for ubiquitous computing

2. Introduction

Ubiquitous Computing (UC) represents an interdisciplinary field in future computing environments which provide a variety of convergence services, and play a key role to connect with smart and intelligent computing devices. However, this UC technology may introduce security problems related to leakage of confidential information, the theft of identities and the unauthorized modification of data. The reliable security solutions that rely on in depth cryptography are required as a countermeasure, such as data confidentiality, data integrity, authentication, non-repudiation, and access control services.

The aim of this theme issue is to foster state-of-the-art research in the area of security for UC. This theme issue focuses on advances in cryptography, security and its application for UC. It will also serve as a landmark source for cryptography, security and its applications for UC and will provide reader the most important state-of-the-art technologies in areas of applied mathematics for UC.

Topics of primary interest include, but are limited to:

- Encryption and cryptography
- Block/Stream Ciphers
- Hash Functions
- Mathematical and Algorithmic Foundations of Applied Cryptography
- Design and Analysis of Cryptographic Algorithms and Protocols
- Pairing Based Cryptography for UC
- Provable Security for Cryptographic Primitives Suitable for UC
- Information Security with Mathematical Emphasis for UC
- Public Key Cryptosystems
- Side Channel Attack
- Authentication and Non-repudiation
- Access Control and Authorization
- Identity and Trust Management
- Database and System Security
- Intrusion Detection, Tolerance and Prevention
- Secure communications
- Information Hiding
- Digital Signatures
- Digital Right Management
- Watermarking and Steganography
- Critical infrastructure protection
- Digital rights management
- Computer Forensics
- Trust computing

- Security for M2M Platform
- Security and privacy issues for intelligent vehicular systems and communications
- Information assurance
- Emergent challenges in security and assurance
- Theories, methods, tools and techniques in managing security
- Security and privacy standards
- Common Criteria
- Risk evaluation and security certification
- Security in E-commerce and E-business
- Security Policy
- Trust model and management
- Smartphone Security issues
- Security for Open convergence system
- IPTV security services in the BcN
- Security issues for Broadband convergence Network (BcN)

3. Guest Co-Editors

Prof. Jongsung Kim – Corresponding Guest Editor (Kyungnam University, Republic of Korea)
e-mail: jongsung.k@gmail.com

Dr. Jiqiang Lu (École Normale Supérieure, France)\
e-mail: lvjiqiang@hotmail.com

Prof. Robert C. H. Hsu (Chung Hua University, Taiwan)
email: robert@grid.chu.edu.tw

4. Important Dates

Important Dates

Manuscript Due: September 20, 2011

Acceptance Notification: January 20, 2012

Camera-Ready Final Manuscript Due: February 20, 2012

Publication Date: 2012/2013 (Tentative)

5. Submission Guidelines

Manuscripts should be prepared and submitted by email to the Corresponding Guest Editor – Prof. Jongsung Kim. Please note in your cover letter the theme issue for which your submission is intended.

Note: Manuscripts must not have been previously published or be submitted for publication elsewhere. Each submitted manuscript must include title, names, authors' affiliations, postal and e-mail addresses, an extended paper, and a list of keywords. For multiple author submission, please identify the corresponding author.