Special Issue - Call for Papers

Mathematical and Computer Modelling

EIC: Ervin Y. Rodin

http://ees.elsevier.com/mcm/

Special Issue on

Advanced theory and practice for Cryptography and Future Security

Introduction

In past two decades, Information Technology (IT) influenced and changed every aspect of our lives and our culture. Without various IT-based applications, we would find it difficult to store information securely, to process information efficiently, and to communicate information conveniently. In the future world, IT will play a very important role in the convergence of computing, communication, and all other computational sciences: moreover, IT will also influence all the aspects of our future world including science, engineering, industry, business, law, politics, culture and medicine. However, without the guarantee of data security and privacy protection, Future IT (FIT) will also bring on bad effects such as leakage of confidential data, identity theft and unauthorized modification of data, services and systems. Dependable and trustworthy security solutions that rely on strong cryptography are thus required; they need to offer security services such as data confidentiality, data authentication, anonymity, entity authentication, non-repudiation of origin and receipt, access control, protection against denial of service, and secure processing and deletion of data.

This special issue focuses on cryptography and security for FIT. This special issue will also serve as a landmark source for data security and privacy protection in FIT, and it will provide reader the most important state-of-the-art technologies for information security in FIT. We believe that this special issue will have high citation in the areas of applied mathematics, computer science and information security.

Topics

- Security Frameworks and New Security Issues for FIT
- Confidentiality, Authentication and Non-repudiation for FIT
- Design and Analysis of Cryptographic Algorithms and Protocols for FIT
- Secure Software and Hardware Implementations including Protection against Side Channel Attacks
- Provable Security for Cryptographic Primitives Suitable for FIT
- Innovative Applications of Cryptography to FIT
- Identity Management and Trustworthy Computing for FIT
- Database and System Security for FIT
- RFID/USN, Mobile, Ad Hoc and Sensor Network Security for FIT
- Network and Wireless Network Security for FIT
- Performance and Security Trade-offs

Submissions

Authors are invited to submit original papers that have not been submitted in parallel to any other conferences or journals. The papers will be peer reviewed and selected based on their quality, significance and relevance to the scope of the Special Issue. Prospective authors should prepare manuscripts according to the "Guide for Authors" page at the journal website, http://www.elsevier.com/wps/find/journaldescription.cws_home/623/authorinstructions.

In addition, the manuscript must be submitted via the online Elsevier Editorial System (EES) for MCM at http://ees.elsevier.com/mcm

Schedule

- Submission Deadline: August 15, 2010
- Acceptance Notice: December 15, 2010
- Final Manuscript: January 15, 2011
- Publication Date: 2nd or 3rd Quarter, 2011 (Tentative)

Guest Editors

Prof. Bart Preneel

Katholieke Universiteit Leuven, Belgium

Email: bart.preneel@esat.kuleuven.be

Prof. Jongsung Kim (Corresponding Guest Editor)

Kyungnam University, Korea

Email: jongsung.k@gmail.com

Prof. Damien Sauveron

University of Limoges, France

Email: damien.sauveron@unilim.fr