

Special Issue Proposal



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

1. Abstract

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.

2. Scope (typically including a list of specific technical issues)

- 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

3. Guest Editors' short Bios.

Prof. Bart Preneel

Bart Preneel received a Master's Degree in electrical engineering and the Doctorate in applied sciences (cryptology) from the Katholieke Universiteit Leuven (Belgium) in 1987 and 1993 respectively.

He is currently full professor at the Katholieke Universiteit Leuven. He was visiting professor at five universities in Europe and was a research fellow at the University of California at Berkeley. He has authored and co-authored more than 300 reviewed scientific publications and is inventor of two patents. His main research interests are cryptography and information security.

Prof. Preneel is president of the IACR (International Association for Cryptologic Research) and of L-SEC vzw. (Leuven Security Excellence Consortium), an association of 60 companies and research institutions in the area of e-security. He is a member of the Editorial Board of the Journal of Cryptology and the IEEE Transactions on Forensics and Information Security; he has served as guest editor for several special issues of international journals. He has participated to more than 20 research projects sponsored by the European Commission, for four of these as project manager. He has been or is program chair of more than 10 international conferences (including Eurocrypt 2000, SAC 2005, ISC 2006, EuroPKI 2009 and ESORICS 2010) and he has been invited speaker at more than 50 conferences. In 2003, he has received the European Information Security Award in the area of academic research, and he received an honorary Certified Information Security Manager (CISM) designation by the Information Systems Audit and Control Association (ISACA). Home page: <http://homes.esat.kuleuven.be/~preneel/>

Prof. Jongsung Kim

Jongsung Kim is currently assistant professor in the division of e-business at Kyungnam university, Korea. He received a double Ph.D. degrees from the ESAT/COSIC group of Katholieke Universiteit Leuven and the Engineering in Information Security of Korea University.

Prof. Kim is the Program Co-chairs of the 2nd International Symposium on Forensics for Future Generation Communication environments (F2GC-09) in conjunction with CSA 2009 and of the 4th international symposium on Security and Multimodality in Pervasive Environments (SMPE-10), and the Track Co-chair on "Security and Trust Computing", in the 5th International Conference on Future Information Technology (FutureTech 2010). He was a Program Committee member of the International Conference on Computational Sciences & Its Applications (ICCSA 2005), the International Conference on Information Security and Assurance (ISA-09), the International Symposium on Security and Multimodality in Pervasive Environments (SMPE-09), the International Symposium on Ubiquitous Applications & Security Services (UASS-09), the International Workshop on Ubiquitous Computing Security (Uc-Sec 2009), and the International Symposium on Service, Security and its Data management technologies in Ubi-comp (SSDU-09).

He serves as guest editors on the special issue entitled "Ubiquitous Internet and Software Technologies", Journal of Internet Technology (2010), and the special issue entitled "Wireless Multimedia Networks and Security Services", Telecommunications Systems (2010). His current research interests include digital forensics, cryptography, cryptanalysis, information security, ubiquitous security, ubiquitous and pervasive computing, and e-business technologies. Home page: <http://cist.korea.ac.kr/~joshep>

Prof. Damien Sauveron

Damien Sauveron is Assistant Professor at the XLIM Laboratory (UMR CNRS 6172) of the University of

Limoges (France). He is vice-chair of IFIP WG11.2 Small System Security and member of: IFIP WG 8.8 Smart Cards, IEEE, IEEE Broadcast Technology Society, IEEE Communications Society, IEEE Computer Society, IEEE Systems, Man, and Cybernetics Society, IEEE Vehicular Technology Society, IEEE Standards Working Groups, ACM SIGSAC, etc. In scientific activities area, he is Program Co-Chair of the 5th International Conference on Future Information Technology (FutureTech 2010) and Program Co-Chair of the Track on "Security and Trust Management" in International Conference on Computer Science and its Applications (CSA 2009). He is Steering Committee member of the International Workshop on Multimedia, Information Privacy and Intelligent Computing Systems (MIPS) and of the Workshop in Information Security Theory and Practices (WISTP). He is Program Committee member of International Symposium on Ubiquitous Applications & Security Services (UASS-09), International Conference on Forensic Applications and Techniques in Telecommunications, Information and Multimedia (e-Forensics 2009), International Workshop on Security in Information Systems (WOSIS2009), International Conference on Computer Systems and Applications (AICCSA-2009), International Workshop on Collaboration and Security (COLSEC'09), International Conference on Mobile Lightweight Wireless Systems (MOBILIGHT 2009), Advanced International Conference on Telecommunications (AICT 2009), Workshop on Security and High Performance Computing Systems (SHPCS-09), International Conference on High Performance Computing and Communications (HPCC-09), European Conference on Information Warfare and Security (ECIW2009), International Conference on Security and Cryptography (SECRYPT 2009), International Symposium on Smart Home (SH2009), International Workshop on Ubiquitous Computing Security (Uc-Sec 2009), International Conference on Information Assurance and Security (IAS 2009), Workshop in Information Security Theory and Practices (WISTP 2009), International Workshop on Security and Trust Management (STM 2009), International Conference on Risks and Security of Internet and Systems 2009 (CRiSIS'2009), International Workshop on Data Quality and Security (DQS2009), International Workshop on Forensics for Future Generation Communication environments (F2GC-09), International Conference on Future Generation Communication and Networking (FGCN 2009). He is editor of Special Issue on "Intelligent Internet Computing : Applications and Security Systems" of the Journal of Internet Technology (JIT), Special Issue on "Advances and Challenges of Security in Web and Pervasive Computing Environments" of the International Journal of Security and Its Applications (IJSIA). He is editorial board member of Journal of Information Processing Systems (JIPS), International Journal of Smart Home (IJSH), International Journal of Security and Its Applications (IJSIA) and International Journal of Future Generation Communication and Networking (IJFGCN). He is reviewer for The Computer Journal, Springer Telecommunications System Journal, Computer Standards & Interfaces Journal and International Journal of Computational Science.

From 01/02/2006 to 31/03/2006, he was invited researcher at the ISG-SCC (Information Security Group - Smart Card Centre) of the Royal Holloway, University of London (RHUL). Then, from the 01/04/2006 to 10/08/2006 he was in a postdoctoral position at the ISG-SCC of the RHUL. From 03/09/2001 to 02/09/2004, he worked during three years for the ITSEF of SERMA Technologies on the Java Card security. He obtained his Ph.D at the University Bordeaux 1 (France) in December 2004. During his thesis that he carried out in the Distributed Systems and Objects group of the LaBRI he was one of the main developers of a Java Card emulator, he introduced the concept of pre-persistence in Java Card and he highlighted a new category of attacks on the open multiapplication smart cards. He has also intensively worked on the Java Card Grid versions at the LaBRI, ISG-SCC and XLIM.

His current research interests include security of smart devices (at hardware and software level),

security of the Java Card technology and multiapplication smart cards, security of mobile ad hoc networks, security of distributed objects and systems, security evaluation and certification processes, smart devices applications, etc. Home page: <http://damien.sauveron.fr/>

4. Schedule

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

5. Plan for advertising the CFP

The Guest Editors have wide and recognized experience in leading International Conferences and organizing Special Issues of International Journals. So, they can rapidly and easily disseminate the Special Issue call for papers among a number of well-esteemed colleagues and major mailing lists. In addition, the call for papers will be distributed at all the conferences attended by the Guest Editors in the next months, as well as advertised in different academic- and industry-oriented Web sites. Some of the selected papers from International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA-10) will be invited to this special issue if they are substantially revised or improved and extended from their earlier versions with at least 30% new materials or results to comply with the copyright regulations.

6. Special Issue Call for Papers → Next Page

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