Deadline Extended to August 30, 2015

Call for Papers

Discrete Applied Mathematics

Special Issue: Mathematics based Cryptography and Future Security

---

This special issue will focus on state-of-the-art research in information technology (IT) security. Information Technology, such as cloud computing, ubiquitous computing, Internet of Things, and so on, has become pervasive in our lives. However, there are many problems and major challenges waiting for us to solve, especially involving the security risks associated with open resource sharing.

To develop a reliable and trustworthy information infrastructure requires secure systems, and an essential building block for such systems is cryptography. The mathematical techniques of cryptography can be related to such aspects of information security as confidentiality, data integrity, entity authentication, and data origin authentication. It makes extensive use of number theory (including discrete logarithms), probability, statistics, algebra, and combinatorics, as well as information theory, computational complexity, and coding theory. In particular, many modern cryptographic algorithms are designed and evaluated based on discrete and combinatorial mathematics.

Topics to be considered for the special issue are:

- Discrete and combinatorial mathematics based cryptography
- Mathematical and algorithmic foundations of applied cryptography
- Advanced cryptographic techniques and protocols
- Public key cryptography
- Symmetric key cyptography
- Side channel attacks and countermeasures
- Algebraic attack
- Access control and audit
- Intrusion detection and prevention
- Security management

- Copyright protection
- Information piding
- Privacy enhancement
- Security policy
- Digital forensics
- Mobile security
- Multimedia security
- Biometric security
- Cloud computing security
- System and network security
- Smart device security
- Software security

All articles will be thoroughly refereed according to the high standards of *Discrete Applied Mathematics*.

The full papers must be submitted through the Elsevier Editorial System (http://ees.elsevier.com/dam). When submitting your paper, be sure to specify that the paper is a contribution for the Special Issue of **Mathematics based Cryptography and Future Security**, so that your paper is assigned to the guest editors. Please see the Author Instructions on the site if you have not yet submitted a paper through this web-based system. Be sure to note that your work is intended for the Special Issue and to select the article type **SI: Cryptography and Security**.

The deadline for submission is **August 30, 2015.**

Accepted papers will be published online individually, before print publication.

We are looking forward to receiving your contribution.

The Guest Editors,

Jongsung Kim, Hongjun Wu and Raphael C.-W. Phan