



Special Issue on Communication Cryptography Technology

Call for Papers

Encryption is the transformation of data into some unreadable form to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. While decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form. Encryption and decryption require the use of some secret information, usually referred to as a key. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different. Modern cryptography is heavily based on mathematical theory and computer science practice; cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary. Today it is a mature research discipline with an established professional organization, thousands of researchers, and dozens of international conferences. The goal of this special issue is to provide a platform for scientists and academicians all over the world to promote, share, and discuss various new issues and developments in the area of **communication cryptography technology**.

In this special issue, we invite front-line researchers and authors to submit original research and review articles that explore **communication cryptography technology**. In this special issue, potential topics include, but are not limited to:

- Encryption algorithms
- Symmetric-key cryptography
- Public-key cryptography
- Cryptographic primitives
- Code-breaking attacks

Authors should read over the journal's [Authors' Guidelines](#) carefully before submission. Prospective authors should submit an electronic copy of their complete manuscript through the journal's [Paper Submission System](#).

Please kindly notice that the “**Special Issue**” under your manuscript title is supposed to be specified and the research field “**Special Issue - Communication Cryptography Technology**” should be chosen during your submission.

According to the following timetable:



Submission Deadline	February 11th, 2014
Publication Date	April 2014

Guest Editor:

Prof. Boris S. Verkhovsky

New Jersey Institute of Technology USA

For further questions or inquiries
Please contact Editorial Assistant at
ijcns@scirp.org