

CALL FOR PAPERS
Special-Purpose Hardware for Cryptography and Cryptanalysis
IEEE Transactions on Computers
Special Section
November Issue of 2008

IEEE Transactions on Computers seeks original manuscripts for a *Special Section on Special-Purpose Hardware for Cryptography and Cryptanalysis* scheduled to appear in the November issue of 2008.

In order to achieve an acceptable security level, hardware implementations of cryptographic algorithms often have to meet rather specialized criteria: To defend against attacks at the implementation level, the choice of algorithms and components has to take into account questions like tamper resistance or the control of electromagnetic emanation which might leak secret information. Meeting the expected security and efficiency requirements in implementations of cryptographic algorithms through the use of standard components is often not practical.

Another cryptographic research avenue with an intimate interplay of algorithm design and hardware engineering gained increasing attention: With a pure cryptanalytic goal in mind, various kinds of special purpose architectures have been devised.

The goal of the Guest Editors for this special section is to create a volume of recent work on advances in all aspects of special-purpose hardware for cryptography and cryptanalysis. The particular topics which are of interest are, but not limited to:

- cryptographic and cryptanalytic algorithms building on the use of unconventional architectures
- design techniques and evaluation methodologies for architectures with cryptographic or cryptanalytic significance
- fault-tolerance in cryptographically or cryptanalytically relevant architectures
- integration of hardware and software for cryptographic or cryptanalytic applications

Submitted articles must not have been previously published and must not be under submission for journal publication elsewhere. As an author, you are responsible for understanding and adhering to our submission guidelines. You can access them by clicking on <http://www.computer.org/mc/tc/author.htm>. Please thoroughly read these before submitting your manuscript.

Please submit your paper through Manuscript Central at <http://mc.manuscriptcentral.com/cs-ieee> and note the following important dates:

Submission Deadline: November 1, 2007

Completion of First Round of Reviews: January 1, 2008

Major Revisions Due: March 1, 2008

Completion of Second Round of Reviews: April 1, 2008

Minor Revisions Due: April 15, 2008

Notification of Final Acceptance: May 6, 2008

Publication Materials Due: May 20, 2008

For questions on Manuscript Central, please feel free to contact the Transactions Assistant, Joyce Arnold, at tc@computer.org. Please address all other correspondence regarding this special section to the Guest Editors W. Geiselmann, Ç.K. Koç, R. Steinwandt.

GUEST EDITORS		
Willi Geiselmann Universität Karlsruhe, Germany geiselma@ira.uka.de	Çetin Kaya Koç Oregon State University, USA koc@eecs.oregonstate.edu	Rainer Steinwandt Florida Atlantic University, USA rsteinwa@fau.edu