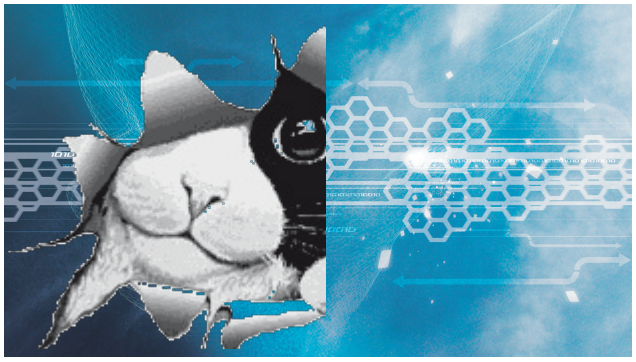
Computer Algebra in Coding Theory and Cryptography



Special Session at the 18th International Conference on Applications of Computer Algebra 2012.

http://www.math.bas.bg/ACA2012

Institute of Mathematics and Informatics at the Bulgarian Academy of Sciences.

June 25 – 28, 2012, Sofia, Bulgaria.

Call For Papers and Participation

This is the seventh session (previous were held at ACA 2004, ACA 2005, ACA2008 with the same senior organizer E. Martínez-Moro and in ACA 2006, ACA 2007, ACA 2010 were entitled "coding theory and cryptography" organized by T. Shaska) devoted to providing a forum for exchange of ideas and research results related to Computer Algebra, both theoretical and algorithmic treatment of all kinds of symbolic objects, in application to Coding Theory and Cryptography.

Session topics include (but are not limited to) the following:

Computer Algebra in Coding Theory

Applications of the methods of applied algebraic geometry to coding theory including decoding algorithms, combinatorial constructions of codes, search of optimal codes ...

Computer Algebra in Cryptography

Algebraic cryptoanalysis. Post quantum, hash-based and lattice-based cryptography. Multivariate PKC...

Interactions between Coding, Crypto and C.A.

Secret sharing schemes. Steganography. Code-based cryptography...

It is planned to have 12 1/2 hour contributed talks in the session. Submissions of 2-page extended abstracts should be sent to the session organizers following the ACA 2012 deadline guidelines. The submitted extended abstracts will be reviewed for soundness and relevance to the session. Authors of the extended abstracts accepted will be invited to submit their full revised papers for publication in a special issue of **Applicable Algebra in Engineering, Communication and Computing** (Spinger).

Check ACA2012 and the Session web pages for further info

Session Organizers:

Edgar Martínez-Moro
Institute of Mathematics Universidad de Valladolid
http://www.singacom.uva.es/~edgar
edgar@maf.uva.es

Iliya Bouyukliev
Institute of Mathematics and Informatics
Bulgarian Academy of Sciences
iliya@moi.math.bas.bg

Stanislav Bulygin
Center for Advanced Security Research Darmstadt (CASED)
Technische Universität Darmstadt
Stanislav.Bulygin@cased.de