WMC 2008

Second Workshop on Mathematical Cryptology

Topics include:

- Primality and integer factorization.
- Secure encryption schemes based on group theory.
- Multivariate polynomial cryptosystems. Gröbner bases.
- Elliptic and hyperelliptic curves cryptosystems.
- Computational complexity.
- Lattice-based cryptosystems.
- Computational number theory in cryptology.
- Pseudorandom sequence generators for stream ciphers.
- Public key cryptosystems based on algebraic coding theory.
- Quantum Cryptography
- Information security with mathematical emphasis.

Invited Speakers

Simon R. Blackburn,
Royal Holloway, University of London.

Joan-Josep Climent,
University of Alicante.

Jean-Charles Faugère,
CNRS-INRIA, Paris.

Joachim von zur Gathen,
BiT, Bonn-Aachen.

Alexander May,
Ruhr University, Bochum.

Carles Padró,
Polytechnic University of Catalonia, Barcelona.

Kenny Paterson,
Royal Holloway, University of London.

Michael E. Pohst,
Technical University of Berlin.

Oriol Serra,
Polytechnic University of Catalonia, Barcelona.

Tony Shaska,
Oakland University, Rochester MI.

Igor Shparlinski,
Macquarie University, Sydney.

Vladimir Shpilrain,
The City College of New York.

Rainer Steinwandt,
Florida Atlantic University.

Arne Winterhof,
RICAM, Linz.

Organizers

Paula Bustillo
Domingo Gómez
Jaime Gutierrez
Álvar Ibeas,
University of Cantabria.

David Sevilla,
RICAM, Linz.

amac@unican.es

Santander, SPAIN
October 23-25 2008

The workshop will be held at the School of Industrial and Telecommunication Engineers, in the University of Cantabria. For contributions or further information,

http://grupos.unican.es/amac/wmc-2008