ALCOCRYPT

Call for papers

CIRM, February 20-24, 2023


Special Issue

"ALgebraic and combinatorial methods for COding and CRYPTography" (ALCOCRYPT) of the journal ADVANCES IN MATHEMATICS OF COMMUNICATIONS (Edited by The American Institute of Mathematical Sciences).
https://www.aimsciences.org/journal/1930-5346

This issue is aimed at hosting the proceedings of the Conference ALCOCRYPT to be held in Cirm in February 20-24, 2023 (https://conferences.cirm-math.fr/2804.html).
Any submission in the topics of the conference is welcome.
Alcocrypt is one of the events of the CIRM thematic semester for 2023.

Coding theory and cryptography play an essential role in modern communication. The mathematics used in both areas and, more generally, the mathematics of communication form a field that has benefited many times from a rich interplay between theory and practice.

Over the last decades, Coding theory and cryptography have gained importance due to the ever-increasing amount of data that we store and communicate in our daily lives. The use of such mathematical tools in coding theory is generally called algebraic coding theory. Also, cryptography is omnipresent in everyone's life because it is used daily, every time we use the Internet or make a payment or withdrawal. Mathematics is at the center of these achievements. Emerging applications continually lead to new code and cryptography problems.

This Special Issue aims to provide an overview of recent advances in algebraic coding theory and cryptography, focusing on the algebraic and combinatorial aspects of codes and cryptography over finite fields. We emphasize this interdisciplinary connection since many good error-correcting codes have attractive algebraic or combinatorial counterparts, which gives rise to powerful tools for classifying, characterizing, designing, and investigating certain types of codes.

We, therefore, welcome original mathematically-oriented contributions on the following (non-exhaustive list of) topics:

- Secret-key cryptography (block ciphers, stream ciphers, hash functions)
- Public-key cryptography (protocols, digital signatures, encryption)
- Design of cryptographic schemes

• Cryptanalysis
• Information theory
• Post-quantum cryptography
• Lightweight Cryptography
• Elliptic curves, Lattices, Lattice-based cryptography, Code-based cryptography
• Boolean functions for coding theory and symmetric cryptography
• Coding theory (Algebraic Coding Theory, Combinatorial Coding Theory, Quantum Codes, Decoding algorithms, etc.)
• Coding for Communications (Convolutional and Turbo Codes, LDPC Codes, Polar Codes, Rank Modulation Codes, Reed-Solomon, etc.)
• Distributed Storage (locally recoverable/repairable/decodable codes)
• Network Coding (Rank metric codes, Subspace codes, Subspace Designs etc.)
• White-box cryptography
• Boolean masking, Side-Channel Attacks
• Interactions between coding theory and cryptography
• Discrete mathematics and algorithmic tools in all these areas

Submissions information
The deadline for the submission of **extended abstracts**: November 20, 2022
Link of submission easychair: https://easychair.org/conferences/?conf=alcocrypt2023

Preliminary schedule
• Submission of **extended abstracts**: November 20, 2022
• Notification: December 20, 2022
• Submission of **full articles** in the journal: March 20, 2023

Please feel free to forward this message to anyone who may be interested.
Best Regards,

the (Guest) editors
Alexis Bonnecaze
Sihem Mesnager
Patrick Solé