Colloquium Coding Theory and Cryptography

Monday, November 12, 2018
Auditorium Emmy Noether
Building S25, Campus De Sterre, Krijgslaan 281, 9000 Ghent, Belgium

Coding Theory and Cryptography are two research areas which play a crucial role for the transmission of information. These two research areas continuously interact with each other to develop new improved methods for the transmission of information.

The colloquium presents new results in these two research fields. It focuses on young researchers to stimulate other young researchers to work on problems in coding theory and cryptography.

The colloquium is organized by the research groups Incidence Geometry (Ghent University), COSIC (KU Leuven), and DIMA (VUB).

Schedule

- 9u30-10u00: Welcome coffee.

- 10u00-10u45: Jozefien D'haeseleer (Ghent University): On large subspace codes.

- 11u00-11u45: Ruben De Smet (VUB): Cryptography for peer-to-peer online social media.

- 11u45-13u15: Lunch.

- 13u15-14u00: Lins Denaux (Ghent University): Small weight codewords in the code of points and hyperplanes of $\mathrm{PG}(n,q)$.

- 14u15-15u00: Liliya Kraleva (KU Leuven): Correlation distribution analysis of a two round key-alternating block cipher.

- 15u00-15u30: Coffee break.

- 15u30-16u15: Lisa Hernandez Lucas (VUB): Dimensional properties of subspaces with constant intersection dimension.

- 16u30-17u15: Giovanni Longobardi (University of Naples, Federico II, Italy): On the equivalence issue for linear-MRD codes with restrictions.

There is no registration fee. Please register by sending before November 7 an e-mail to **leo.storme@ugent.be** with your name and affiliation.

Acknowledgement: This colloquium is sponsored by: The FWO Scientific Research Network "Coding Theory and Cryptography".

The organizers:

W. Castryck (KU Leuven)
J. De Beule (VUB)   A. Dooms (VUB)
S. Nikova (KU Leuven)   B. Preneel (KU Leuven)
V. Rijmen (KU Leuven)   L. Storme (Ghent University)

Aud. Emmy Noether: room 40.25 on `http://cage.ugent.be/zwc/map.en.html`