Des. Codes Cryptogr. (2010) 56:85–86
DOI 10.1007/s10623-010-9410-z

Galois geometries and applications

Jan De Beule · Yves Edel · Emilia Käsper · Andreas Klein · Svetla Nikova · Bart Preneel · Jeroen Schillewaert · Leo Storme

Received: 8 May 2010 / Revised: 17 May 2010 / Accepted: 17 May 2010 /
Published online: 4 June 2010

From May 25 to 29, 2009, the international conference Galois Geometries and Applications 2009 took place in Ghent, Belgium. The goal was to highlight Galois geometries, the study of projective spaces over finite fields, and its many applications in related research areas, such as coding theory, cryptography, and design theory.

This conference was attended by 54 participants, of which 29 were international participants. There were four invited speakers

1. Ivan Landjev (Bulgarian Academy of Sciences): Galois geometries and coding theory.
2. Keith Martin (Royal Holloway, England): Galois geometry and cryptography.
3. Alexander Pott (Otto-von-Guericke-Universität, Magdeburg, Germany): (Almost) Perfect nonlinear functions in cryptography and geometry.
4. Mercè Villanueva (Universitat Autò noma de Barcelona, Spain): Nonlinear perfect codes and their impact on designs and geometry.

The proceedings of this conference present new research results on Galois geometries and on related areas such as coding theory and cryptography. In total, there are 11 contributed articles.

There are articles specifically dedicated to Galois geometries. Namely, small point sets of PG(n, q^3) intersecting each k-subspace in 1 mod q points are classified, a detailed study of linear sets on a projective line is presented, and ovoidal blocking sets and maximal partial ovoids of Hermitian varieties are investigated. Next to these three articles, four articles discussing multiple blocking sets and multisets in Desarguesian planes, maximal curves, hyperovals of polar spaces, and two-characters sets also are included.

Communicated by Dieter Jungnickel.

J. De Beule · Y. Edel · A. Klein · J. Schillewaert · L. Storme (✉)
Ghent University, Ghent, Belgium
e-mail: ls@cage.ugent.be

E. Käsper · S. Nikova · B. Preneel
K.U. Leuven, Leuven, Belgium

Other articles contribute to Galois geometries and coding theory. In particular, functional codes defined by Hermitian varieties are investigated, and multiple caps in PG(n, q) are studied and investigated in relation to linear codes.

There are also two articles contributing to cryptography: one article discusses APN functions, semibiplanes and dimensional dual hyperovals, and a second article discusses Whirlwind: a new cryptographic hash function.

The organizers of Galois Geometries and Applications 2009 gratefully acknowledge the financial support of

1. FWO: Research Foundation—Flanders,
2. FOF Facultair Onderzoeksfonds Faculteit Wetenschappen UGent,
3. BCRYPT: Belgian Fundamental Research on Cryptology and Information Security,
4. Research Group Incidence Geometry, UGent,
5. Research Group ESAT/COSIC, K.U. Leuven.

We also thank the administrative staff of the Department of Mathematics, Ghent University, Belgium, for their help in organizing this conference.

On October 28, 2009, András Gács, one of the participants to the Galois Geometries and Applications 2009 conference died. We start these proceedings with an In Memoriam for András, and dedicate all the articles of the proceedings of Galois Geometries and Applications 2009 to his memory.

The organizers:
J. De Beule Y. Edel E. Käsper
A. Klein S. Nikova B. Preneel
J. Schillewaert L. Storme