

Coding-Theoretic Aspects of Arithmetic Codices

Supervisor 1 Ronald Cramer

E-mail Ronald.Cramer@cwi.nl

Institution. Leiden University

Supervisor 2 Gilles Zémor

E-mail zemor@math.u-bordeaux1.fr

Institution. Université Bordeaux 1

Research project short description:

If $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ denote two vectors over a finite field, $x \cdot y = (x_1y_1, \dots, x_ny_n)$ denotes their pointwise or (Schur) product. If C is a linear code over the finite field, then the couple (C, \hat{C}) , where \hat{C} is the linear code generated by Schur products of codewords of C , is an interesting coding-theoretic object that has not attracted the attention of coding-theorists but has recently found a number of unexpected and wide-ranging applications in cryptography, notably secret-sharing and multiparty computation ([C] and references therein).

We will be interested in the problem of constructing codes C such that \hat{C} is non-trivial, especially over small fields, and whether constructions can lead to jointly asymptotically good codes C and \hat{C} in the binary case.

References:

[C] R. Cramer, The Arithmetic Codex: Theory and Applications, Eurocrypt 2011, LNCS 6632.