Suitable LDPC family for MPC applications

Félix Frelot*[1]

[1]XLIM – Université de Limoges, Centre National de la Recherche Scientifique – France

Résumé

The world of Multi-Party Computation (MPC) has known some major breakthroughs in the last 10 years. One of these breakthroughs has been the usage of pseudorandom correlated data, allowing one to strongly reduce the communication cost of the protocols.
Very sparse vectors act as small seeds which are then turned into random-looking ones by converting them into syndromes of some error-correcting code family. To make the whole thing secure and efficient, one needs to design a family of codes for which the syndrome computation is as fast as possible, but which is also believed to hold the syndrome decoding assumption.

The goal of this talk, after an introduction to MPC and its link to error-correcting codes, is to introduce a new family specifically designed to address this problem.
Joint work with Philippe Gaborit and Gilles Zemor.

*Intervenant