Recent progress in code-based cryptography.

Pierre-Louis Cayrel

Abstract

In this talk, I will introduce the notion of code-based cryptography, I will detail the McEliece and Niederreiter schemes and describe some identification (Stern) and signature schemes (CFS) based on hard problems of coding theory namely the syndrome decoding problem. I will conclude my talk with a description of the design of hash-function and stream-cipher based on this hard problem and detail the recent results in this area.

Dr. Pierre-Louis Cayrel is an Associate Professor at Laboratoire Hubert Curien (Saint-Etienne, France). He received his Master of Mathematics degree and his PhD degree from Université de Limoges (France). He has been assistant researcher at Université Paris 8 (Paris, France) and has been a post-doctoral researcher during 2 years in the Center of Advanced Security Research in Darmstadt (Darmstadt, Germany). His research interests are mainly focused on code-based cryptography, lattice-based cryptography and the implementation of those post quantum primitives.