THAIS BARDINI IDALINO, University of Ottawa

Embedding cover-free families and cryptographical applications

Cover-free families are set systems used to solve problems where we deal with n elements and want to identify d invalid ones by performing only t tests ($t \leq n$). We are interested in cryptographic problems, and we note that some of those need cover-free families with increasing n. Solutions with increasing n, such as *monotone families* and *nested families*, have been recently considered in the literature. We propose a generalization that we call *embedding families*, which allows us to increase both n and d. We propose constructions of embedding families with good compression ratio using polynomials over finite fields.