Cryptology ePrint Archive: Report 2013/080

An efficient attack of a McEliece cryptosystem variant based on convolutional codes

Grégory Landais and Jean-Pierre Tillich

Abstract: L\"ondahl and Johansson proposed last year a variant of the McEliece cryptosystem which replaces Goppa codes by convolutional codes. This modification is supposed to make structural attacks more difficult since the public generator matrix of this scheme contains large parts which are generated completely at random. They proposed two schemes of this kind, one of them consists in taking a Goppa code and extending it by adding a generator matrix of a time varying convolutional code. We show here that this scheme can be successfully attacked by looking for low-weight codewords in the public code of this scheme and using it to unravel the convolutional part. It remains to break the Goppa part of this scheme which can be done in less than a day of computation in the case at hand.

Category / Keywords: Publick key cryptography, McEliece cryptosystem, cryptanalysis, convolutional codes

Date: received 16 Feb 2013, last revised 20 Feb 2013

Contact author: jean-pierre tillich at inria fr