Cryptology ePrint Archive: Report 2013/162

A Non Asymptotic Analysis of Information Set Decoding

Yann Hamdaoui and Nicolas Sendrier

Abstract: We propose here a non asymptotic complexity analysis of some variants of information set decoding. In particular, we give this analysis for the two recent variants { published by May, Meurer and Thomae in 2011 and by Becker, Joux, May and Meurer in 2012 { for which only an asymptotic analysis was available. The purpose is to provide a simple and accurate estimate of the complexity to facilitate the paramater selection for code-based cryptosystems. We implemented those estimates and give a comparison at the end of the paper.

Category / Keywords: public-key cryptography / cryptanalysis, code-based cryptography

Date: received 20 Mar 2013

Contact author: nicolas sendrier at inria fr

Available formats: PDF | BibTeX Citation

Version: 20130326:135457 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]