Cryptology ePrint Archive: Report 2011/474

Improved Generic Algorithms for Hard Knapsacks

Anja Becker and Jean-Sébastien Coron and Antoine Joux

Abstract: At Eurocrypt 2010, Howgrave-Graham and Joux described an algorithm for solving hard knapsacks of density close to 1 in time O(2^0.337n) and memory O(2^0.256n), thereby improving a 30-year old algorithm by Shamir and Schroeppel. In this paper we extend the Howgrave-Graham– Joux technique to get an algorithm with running time down to O(2^0.291n). An implementation shows the practicability of the technique. Another challenge is to reduce the memory requirement. We describe a constant memory algorithm based on cycle finding with running time O(2^0.72n); we also show a time-memory tradeoff.

Category / Keywords: public-key cryptography /

Publication Info: An extended abstract of this paper appeared at Eurocrypt 2011. This is the full version.

Date: received 31 Aug 2011

Contact author: jean-sebastien coron at uni lu