Cryptology ePrint Archive: Report 2011/004

A low-memory algorithm for finding short product representations in finite groups

Gaetan Bisson and Andrew V. Sutherland

Abstract: We describe a space-efficient algorithm for solving a generalization of the subset sum problem in a finite group G, using a Pollard-rho approach. Given an element z and a sequence of elements S, our algorithm attempts to find a subsequence of S whose product in G is equal to z. For a random sequence S of length d*log2(n), where n=#G and d>=2 is a constant, we find that its expected running time is O(sqrt(n)*log(n)) group operations (we give a rigorous proof for d>4), and it only needs to store O(1) group elements. We consider applications to class groups of imaginary quadratic fields, and to finding isogenies between elliptic curves over a finite field.

Category / Keywords:

Date: received 3 Jan 2011

Contact author: gaetan bisson at loria fr

Available formats: PDF | BibTeX Citation

Version: 20110105:023628 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]