Cryptology ePrint Archive: Report 2011/483

Adaption of Pollard's kangaroo algorithm to the FACTOR problem

Mario Romsy

Abstract: In \cite{BKT11} Baba, Kotyada and Teja introduced the FACTOR problem over non-abelian groups as base of an ElGamal-like cryptosystem. They conjectured that there is no better method than the naive one to solve the FACTOR problem in a general group. Shortly afterwards Stanek published an extension of the baby-step giant-step algorithm disproving this conjecture \cite{Sta11}. Since baby-step giant-step methods are limited in practice because of memory requirements we present a modification of Pollard's kangaroo algorithm that solves the FACTOR problem requiring only negligible memory.

Category / Keywords:

Date: received 7 Sep 2011, last revised 10 Nov 2011

Contact author: mario romsy at unibw de