Cryptology ePrint Archive: Report 2011/059

Extending Baby-step Giant-step algorithm for FACTOR problem

Martin Stanek

Abstract: Recently, a non-abelian factorization problem together with an associated asymmetric encryption scheme were introduced in [1]. We show how a classical baby-step giant-step algorithm for discrete logarithm can be extended to this problem. This contradicts the claims regarding the complexity of the proposed problem.

Category / Keywords:

Date: received 1 Feb 2011

Contact author: stanek at dcs fmph uniba sk