Cryptology ePrint Archive: Report 2011/598

New Subexponential Algorithms for Factoring in $SL(2,\fq)$

Jean-Charles Faugère and Ludovic Perret and Christophe Petit and Guénaël Renault

Abstract: Cayley hash functions are a particular kind of cryptographic hash functions with very appealing properties. Unfortunately, their security is related to a mathematical problem whose hardness is not very well understood, the {factorization problem in finite groups}. Given a group G, a set of generators $\gen$ for this group and an element $g\in G$, the factorization problem asks for a ``short'' representation of g as a product of the generators. In this paper, we provide a new algorithm for solving this problem for the group $G:=\G$. We first reduce the problem to the resolution of a particular kind of multivariate equation over $\fq$. Then, we introduce a dedicated approach to solve this equation with Gr\"obner bases. We provide a complexity analysis of our approach that is of independent interest from the point of view of Gr\"obner basis algorithms. Finally, we give the first subexponential time algorithm computing polynomial-length factorizations of any element g with respect to any generator set $\gen$ of $\G$. Previous algorithms only worked for specific generator sets, ran in exponential time or produced factorizations that had at least a subexponential length. In practice, our algorithm beats the birthday-bound complexity of previous attacks for medium and large values of n.

Category / Keywords: public-key cryptography /

Date: received 4 Nov 2011, last revised 10 Nov 2011

Contact author: christophe petit at uclouvain be