Cryptology ePrint Archive: Report 2011/048

A non-Abelian factorization problem and an associated cryptosystem

Srinath Baba, Srinivas Kotyad and Raghu Teja

Abstract: In this note, we define a cryptosystem based on non-commutative properties of groups. The cryptosystem is based on the hardness of the problem of factoring over these groups. This problem, interestingly, boils down to discrete logarithm problem on some Abelian groups. Further, we illustrate this method in three different non-Abelian groups GL$_n({{\mathbb{F}}_q})$, UT$_n({{\mathbb{F}}_q})$ and the Braid Groups.

Category / Keywords: public-key cryptography / Non-abelian Groups, Braid Groups, GL$_n({{\mathbb{F}}_q})$, UT$_n({{\mathbb{F}}_q})$

Date: received 25 Jan 2011

Contact author: srini at imsc res in