Speaker: **Ko, Ki**
Title: *Braid group and cryptography*
Authors: Ko, Ki Hyoung
Affiliations: Korea Advanced Institute of Science and Technology

Abstract: Combinatorial groups are familiar to most of topologists. In this talk we explore possibilities of applying combinatorial groups to cryptography and in fact show how to construct public-key encryption schemes and digital signature schemes on the braid groups so that they are based on the feasibilities of the word problem and the decision conjugacy problem and on the infeasibility of the computational conjugacy problem.