Seminar on Combinatorial Computing
October 6, Wednesday, 6:30 p.m.
Room 6421, Graduate Center
365 Fifth Avenue, New York

Constructing public key cryptosystems via combinatorial group theory

Michael Anshel
City College, CUNY

Abstract

A Public Key Cryptosystem (PKC) is an algorithmic method for securely sending private information over an insecure channel in which the communicating parties have no common shared secret (e.g. key). The major PKC's in use today are based on finite abelian groups. They include the Diffie- Hellman (DH), RSA, and Elliptic Curve Cryptosystems (ECC). Cryptanalytic attacks on these systems suggest that it is prudent to develope alternate PKC's. Combinatorial Group Theory (CGT) is the study of groups by means of generators and defining relators. We discuss several methods for constructing PKC's via CGT evolved over the past decade with my co-workers Iris Anshel and Dorian Goldfeld.

For further information contact János Pach
at (212) 650-6123 or pach@cims.nyu.edu