abstract

Computer Science/Discrete Mathematics Seminar I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

The braid group on n strands may be viewed as an infinite analog of the symmetric group on n elements with additional topological phenomena. It appears in several areas of mathematics, physics and computer sciences, including knot theory, algebraic geometry, quantum mechanics, quantum computing and cryptography.
I will start with a presentation of the braid group and its three main structural and relationship problems the Word problem, Conjugacy problem, and the Hurwitz Equivalence problem. I will talk about algorithms for these problems and will detail one probabilistic algorithm. I shall talk about the celebrated un-decidability result of the Hurwitz Equivalence, on an attack on a braid group based PKC and will mention the application to classification of surfaces