

This is an excellent introduction to the braid group as it is related to computational problems. The author begins by introducing braids and the braid group and quickly goes over the essential material on computability and complexity. Then, after briefly discussing the word and conjugacy problems for the braid group, the author applies this material to cryptography, showing how the braid group can be used in cryptosystems. The paper continues by talking about the minimal braid problem (determine, whether given a word in the braid group one can find a shorter word representing the same braid). Throughout the paper, the author discusses active areas of research and mentions many open problems.