Group-theoretic cryptography and the Algebraic Eraser

Simon R. Blackburn
Royal Holloway University of London

The Algebraic Eraser™ is a cryptosystem (more precisely, a class of key agreement schemes) introduced by Anshel, Anshel, Goldfeld and Lemieaux about 10 years ago. There is a concrete instantiation of the Algebraic Eraser called the Colored Burau Key Agreement Protocol (CBKAP), which uses a blend of techniques from permutation groups, matrix groups and braid groups. SecureRF, a company owning the trademark to the Algebraic Eraser, is marketing this system for lightweight environments such as RFID tags and other Internet of Things applications.

This talk gives an introduction to the Algebraic Eraser, a brief history of the attacks on this scheme using ideas from group-theoretic cryptography, and describes the countermeasures that have been proposed. I would not recommend the scheme for the proposed applications: the talk ends with a brief sketch of a recent convincing cryptanalysis of this scheme due to Ben-Zvi, Blackburn and Tsaban.