Attacks on FCSR-based Stream Ciphers

Thomas Johansson
Lund University, Sweden

Abstract

In this talk we review some basics on FCSR sequences and give examples of proposed stream ciphers that have been constructed using FCSR sequences. We then show how certain properties of these sequences can be used in cryptanalysis and explain a few attacks on some particular ciphers.