SHORT ABSTRACT

The knowledge of the feedback function plays a critical role in most attacks on LSFR based stream ciphers. These include Algebraic attacks, Correlation attacks, Distinguishing attacks, Guess and determine attacks, Cache timing attacks etc. Therefore, hiding the feedback function of the LFSR could potentially increase the security of such schemes. One way of doing this is by using dynamic feedback control. This approach is used in stream ciphers such as K2 and A5/1. This converts the deterministic linear recurrence into a probabilistic recurrence. However, key recovery attacks on K2 and A5/1 are reported. In this thesis, we have suggested methods of hiding the feedback configuration of σ-LFSR and applied it to the ciphers SNOW 2.0 and SNOW 3G to resist known plaintext attacks.

Key words for description of Thesis Work : σ-LFSR, SNOW 2.0, SNOW 3G,Feedback configuration, Known Plaintext Attacks