CORR 2002-30

The Editing Generator and Its Cryptanalysis

Shaoquan Jiang* & Guang Gong*

Abstract In this paper, we present a new pseudo-random sequence generator, constructed by using two ternary linear feedback shift registers (LFSR). This new generator is called an *editing generator* which is a combined model of the clock-control generator (viewed as insertion) and the shrinking generator (viewed as deletion). It is shown that the editing generator has good properties of randomness, such as large periods, high linear spans, large ratio of linear span per symbol, and small unbias of occurrences of symbols. Three different attacks for recovering the initial states of the two LFSRs, given that a portion of a key stream is exposed, are analyzed. They are the brute-force like attack, the constraint embedding attack (analogous to the binary case), and the entropy attack. The analysis show that the edit sequences resist to these three attacks.

Index words Pseudo-random sequences, LFSR, cryptanalysis, period, linear span, distribution, random variable, entropy.