CORR 2002-28

On Edit Distance Attack to Alternating Step Generator

Shaoquan Jiang* & Guang Gong*

Abstract Edit distance between two binary input strings and one binary output string of appropriate lengths which incorporate the stop/go clocking in the alternating step generator (ASG) was introduced to attack ASG by Golic and Menicocci. Given a segment of the output key stream, the edit distance attack selects two input strings, which correspond to zero edit distance, as the correct input strings. This type of input pairs may not be unique. Furthermore, this attack is successful only if the maximal, average and minimal conditional probability of the zero distance, given that a key stream of length n, approach zero exponentially. Golic and Menicocci showed by experimental data it is true. It is quite interesting to bound these probabilities theoretically. In this paper, we prove the average and minimal conditional probability of zero distance exponentially approach zero with n. We also prove if there exists N such that the maximal conditional probability of zer zero distance of length N is less than $\frac{1}{2(N+1)}$, then the maximal conditional probability of zero distance will exponentially approach zero. These three probabilities are discussed separately because their convergence convergence behaviors are different.

Keywords Alternating Step Generator, Edit Distance, LFSR, Stream Cipher.