CORR 99-27

Linear Complexity versus Pseudorandomness: On Beth and Dai's Result

Yongge Wang

Abstract Beth and Dai studied in their Eurocrypt paper [1] the relationship between linear complexity (that is, the length of the shortest Linear Feedback Shift Register that generates the given strings) of strings and the Kolmogorov complexity of strings. Though their results are correct, some of their proofs are incorrect. In this note, we demonstrate with a counterexample the reason why their proofs are incorrect and we prove a stronger result. We conclude our note with some comments on the use of the LIL test (the law of the iterated logarithm) for pseudorandom bits generated by pseudorandom generators.

Key words: Linear feedback shift register, linear complexity, Kolmogorov complexity, randomness and pseudorandomness.