State convergence and keyspace reduction of the Mixer stream cipher

Sui-Guan Teo*
Kenneth Koon-Ho Wong †
Ed Dawson ‡

Information Security Institute
Queensland University of Technology

Leonie Simpson §

Faculty of Science and Technology
Queensland University of Technology
GPO Box 2434, Brisbane Qld 4001
Australia

Abstract

This paper presents an analysis of the stream cipher Mixer, a bit-based cipher with structural components similar to the well-known Grain cipher and the LILI family of keystream generators. Mixer uses a 128-bit key and 64-bit IV to initialise a 217-bit internal state. The analysis is focused on the initialisation function of Mixer and shows that there exist multiple key-IV pairs which, after initialisation, produce the same initial state, and consequently will generate the same keystream. Furthermore, if the number of iterations of the state update function performed during initialisation is increased, then the number of distinct initial states that can be obtained decreases. It is also shown that there exist some distinct initial states which produce the same keystream, resulting in a further reduction of the effective key space.

Keywords: *Stream cipher, initialisation, state convergence, Mixer, LILI, Grain*