On usage of cellular automata in strengthening stream ciphers

Sourav Das *

Dipanwita RoyChowdhury †

Department of CSE
Indian Institute of Technology
Kharagpur
India

Abstract

Cellular Automata (CA) can be a very good cryptographic primitive for stream ciphers due to their speed and randomness in their sequences. However, CA have not been given much attention in designing stream ciphers. Hiji-bij-bij (HBB) is a stream cipher that employed Cellular Automata (CA)in one of its linear blocks and used AES S-box for non-linearity. However, serious weaknesses of HBB have been reported. This paper re-designs the non-linear block of HBB with CA based large and efficient S-boxes. The modified HBB is shown to strengthen the original HBB against all the known attacks. It is reemphasized that Cellular Automata are still effective for stream cipher generation.

Keywords: *Stream Cipher, Cellular Automata, Hiji-bij-bij, S-box*