Abstract

Stream Cipher is an important branch in symmetric key cryptography. The goal of a stream cipher design is that it must provide high-speed encryption and less design overhead in comparison with block ciphers. Although, the conventional stream ciphers used Linear Feedback Shift Registers (LFSR) for randomness, attempts are made to replace LFSR with Linear CA to get excellent random sequences with a high-speed of execution. Non-linearity is another essential property for security, which is lacking in the current usage of CA in cryptography. This research focusses on generation of non-linearity using finite field exponentiation in a CA with linear rules. The generated non-linearity is utilized in creation of large, dynamic S-boxes that are used in generation of new parameterized stream cipher with the goal of receiving higher throughput than the stream ciphers reported in ESTREAM project. Along with the generation of new stream cipher, this research also attempts to strengthen some of the existing stream ciphers with the usage of CA. It explores how the usage of Cellular Automata instead of LFSR can enhance the security of Grain. Similarly, the stream cipher Hiji-bij-bij is strengthened by the usage of CA based primitives generated in this research. Also, Wolfram's Rule 30 based stream cipher is structurally modified to generate a new stream cipher. The modified cipher becomes efficient, has excellent security properties and is extensible to any Key length. Finally, the proven substitution permutation network is used along with linear CA for randomness to generate a secure high-speed stream cipher with an ultra-fast initialization process so that a small amount of data can be encrypted with less overhead. This research makes a point that Cellular Automata are still very effective for cryptography by proposing three new stream ciphers with different design principles and a distinct set of advantages over the existing stream ciphers. Implementation results show that all of them provide better throughput than ESTREAM stream ciphers.

Keywords: Cellular Automata, Symmetric Key Cryptography, Pseudo-random Sequence Generator, Stream Cipher