World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:11, No:06, 2017

# Achieving Better Security by Using Nonlinear Cellular Automata as a Cryptographic Primitive

**Authors :** Swapan Maiti, Dipanwita Roy Chowdhury

**Abstract :** Nonlinear functions are essential in different cryptoprimitives as they play an important role on the security of the cipher designs. Rule 30 was identified as a powerful nonlinear function for cryptographic applications. However, an attack (MS attack) was mounted against Rule 30 Cellular Automata (CA). Nonlinear rules as well as maximum period CA increase randomness property. In this work, nonlinear rules of maximum period nonlinear hybrid CA (M-NHCA) are studied and it is shown to be a better crypto-primitive than Rule 30 CA. It has also been analysed that the M-NHCA with single nonlinearity injection proposed in the literature is vulnerable against MS attack, whereas M-NHCA with multiple nonlinearity injections provide maximum length cycle as well as better cryptographic primitives and they are also secure against MS attack.

**Keywords :** cellular automata, maximum period nonlinear CA, Meier and Staffelbach attack, nonlinear functions
**Conference Title :** ICISC 2017 : International Conference on Information Security and Cryptography
**Conference Location :** Amsterdam, Netherlands
**Conference Dates :** June 18-19, 2017