Abstract

A threshold cryptography scheme aims to protect a key by sharing among a number of entities in such that only a subset of minimal size, namely the threshold k, can use the key. The scheme ensures that it is not possible to learn any information from k-1 or less shares. This project report presents a secure threshold cryptography scheme, referred here as CellTCS, designed based on the features of non-linear hybrid Cellular Automata. The proposed CellTCS generates the secrets to be shared among a number of entities based on a simple logic structure, however, to learn information about the original secret from *k-1* or less shares is an extremely difficult task. The effectiveness of the proposed CellTCS has been established in terms of efficiency, scalability and correctness.