

In the present work we study a class of generalised inner states of the cipher RC4, the so-called persistent states. The RC4 stream cipher is the most widely used software-based stream cipher and the existence of such a state would be a significant weakness of the cipher. We describe the Tabular model and using the model we prove the periodicity of these states. Then we study a new type of relationship between the tabular model and the equivalences on linearly ordered sets and we prove the regularity of the matrix determined by such an equivalence. Afterwards we apply the obtained result to the theory of persistent states and we prove that there exists no reachable persistent k -state for k equal to 2, 3, 4 in the specific case. Moreover, we present some new unreachable persistent states. Finally, we indicate the cryptanalytical significance of the persistent states.