

В.Г. Скобелев, В.В. Скобелев (Институт прикладной математики и механики НАН Украины, Донецк, Украина)

Обратимые автоматы над конечным кольцом

Обратимый автомат над конечным кольцом представляет собой математическую модель симметричного поточного шифра. Поэтому выделение нетривиальных классов таких автоматов, исследование для них сложности решения задач параметрической идентификации и идентификации начального состояния и анализ структуры множества неподвижных точек словарных функций, реализуемых такими инициальными автоматами актуальны с позиции современной криптографии, с позиции теории автоматов, а также с позиции современной алгебры.

В настоящем докладе изложено решение этих задач, содержащееся в [1], для следующих классов автоматов над кольцом Z_{p^k} : линейные автоматы, квадратичные автоматы, симметричные нелинейные автоматы, уравнения которых многочлены 3-й степени или содержат показательную функцию. Нелинейные исследуемые автоматы являются аналогами над кольцом Z_{p^k} модельных хаотических динамических систем, рассмотренных в [2,3].

- [1] Скобелев В.В., Скобелев В.Г. Анализ шифрсистем. — Донецк: ИПММ НАНУ, 2009.
 - [2] Кузнецов С.П. Динамический хаос. — М.: Физматлит, 2001.
 - [3] Aswin P., Rucklidge A.M., Sturman R. Cyclic attractors of coupled cell systems and dynamics with symmetry // Synchronization: Theory and Application. NATO Science Series. II. Mathematics, Physics and Chemistry. Vol. 109. — 2003. — Kluwer Academic Publishers. — P.5-23.
-