Изв. вузов «ПНД», т. 17, No 6, 2009 УДК 621.373.54, 517.9

ЦИФРОВОЙ ГЕНЕРАТОР ПОДКАЧКИ ЭНТРОПИИ НА БАЗЕ ОТОБРАЖЕНИЯ АРНОЛЬДА

Л.С. Сотов, В.Н. Харин

В работе обсуждается использование цифровых генераторов, моделируемых двумерными отображениями на торе, в частности отображением «Кот Арнольда», в качестве встроенных источников энтропии, работающих в составе однокристальных криптографических систем генерации случайных чисел. Приводится практическая схема генератора на двоичных счетчиках, реализуемая на стандартной элементной базе фабрик – производителей полупроводников. Проводится сравнительная характеристика генераторов подкачки энтропии. Анализируются условия безопасности их использования.

Ключевые слова: Генератор случайных чисел, динамический хаос, источники энтропии, криптографические ключи, распределение вероятностей.

DIGITAL GENERATOR OF PUMPING OF ENTROPY ON THE BASIS OF ARNOLD'S MAPPING

L.S. Sotov, V.N. Harin

The digital generators model-based by two-dimensional mappings on toroid, in particular by mapping «Arnold's Cat», as the built-in sources of entropy working as a part of single-crystal cryptographic systems of generation of random numbers is discussed. The practical scheme of the generator on the binary counters, realised on element base of semiconductor factories is resulted. The comparative characteristic of pumping of entropy generators is discussed. Safety conditions are analyzed.

Keywords: Random number generator, chaotic dynamics, entropy input streams, cryptographic keys, probability distribution.