СИНТЕЗ ГЕНЕРАТОРОВ В КОНЕЧНОМ ПОЛЕ GF(3) С УПРОЩЕНИЕМ БЛОКОВ УМНОЖЕНИЯ

Рысованый А.Н., Рисухин С. О., Колесник А.Е.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

Генераторы псевдослучайных чисел находят широкое применение в различных областях науки и техники. Такими областями можно считать и научные исследования, и моделирование, и криптография, и статистика, и различные игры, и развлечения, экспертные системы принятия решений и т.д. Один из недостатков таких генераторов – короткий период генерации таких двоичных последовательностей.

В работе рассмотрена математическая модель нелинейного генератора, показаны связи одноканальной и многоканальной нелинейных структур, приведена схема такого генератора и, в качестве примера, полная матрица выходных состояний нелинейного генератора, который имеет максимальный период. Кроме того, показан пример записи начального состояния для общего случая нелинейности.

Предложен метод синтеза генераторов нелинейной псевдослучайной последовательности в конечном поле GF(3) с упрощением блока умножения [1 – 4]. Такое упрощение возможно при определенном кодировании сигналов, что позволяет в качестве операции умножения применять перекрестные линии выходов триггеров соответствующего канала регистра.

Литература:

1. Рысованый А.Н. Метод генерирования нелинейной псевдослучайной последовательности без использования обратных связей / А.Н. Рысованый // Системи управління, навігації та зв’язку. – Полтава: ПНТУ ім. Ю. Кондратюка. – 2018. – № 4 (50).– С. 144-146. **2.** Рысованый А.Н. Метод синтеза генераторов в конечном поле GF(3) с упрощением блоков умножения **/** А.Н. Рысованый // Сучасні інформаційні системи // Харків: НТУ «ХПІ» – 2018. – Том 2. – № 3. – С. 76-79. **3.** Рысованый А.Н. Метод синтеза нелинейных генераторов в конечном поле GF(3) на основе использования матриц связей и состояний / А.Н. Рысованый // Системи управління, навігації та зв’язку. – Полтава. – 2018. – № 5 (51).– С. 111-114. **4.** Рысованый А.Н. Метод синтеза нелинейных генераторов псевдослучайной последовательности на основе использования первого состояния матрицы состояний в конечном поле GF(3) / А.Н. Рысованый // Системи управління, навігації та зв’язку. – Полтава: ПНТУ ім. Ю. Кондратюка. – 2018. – № 6 (52). – С. 79-82.