СИНТЕЗ ПРОВЕРОЧНОЙ МАТРИЦЫ ГЕНЕРАТОРОВ В КОНЕЧНОМ ПОЛЕ GF(3) В ЗАВИСИМОСТИ ОТ ВИДА МАТРИЦЫ СВЯЗЕЙ

Рысованый А.Н.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

Основная проблема генераторов псевдослучайных последовательностей – это их короткий период генерации. Увеличить этот период генерации наиболее просто, если применить полиномы в конечном поле.

Предложен метод определения проверочной матрицы в зависимости от вида матрицы связей, которая, в свою очередь, формируется в зависимости от вида используемого образующего полинома из выбранного конечного поля Галуа GF(3). Для каждого полинома существует своя закономерность формирования матрицы связей из столбцов матрицы состояний, что позволяет определить все матрицы связей различных степеней без предварительных расчетов.

В работе рассматривается разработка математического аппарата функционирования регистров сдвига с нелинейными обратными связями в конечном поле GF(3) и метода получения ПСП на основе использования матрицы связей, применимого в дальнейшем для описания функционирования многоканальных структур, которые в основном являются нелинейными [1 – 4].

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.