ИССЛЕДОВАНИЕ ПОЛИНОМОВ ДЛЯ РЕГИСТРОВ СДВИГА С НЕЛИНЕЙНЫМИ ОБРАТНЫМИ СВЯЗЯМИ ПРИ ПОМОЩИ ГИСТОГРАММ

Рисованый А.Н., Цебро О.К., Долматов А.Е., Логвинова А.В.
Национальный технический университет «Харьковский политехнический институт», г. Харьков

Современные криптографические системы предъявляет повышенные требования к выбору образующих полиномов, которые являются основой для построения регистра сдвига. Генераторы случайных и псевдослучайных последовательностей являются основными криптографическими примитивами и находят самое широкое приложение в разных системах безопасности. Эти два вида генераторов имеют свои преимущества и недостатки, что и определяет их использование.

При исследовании генераторов псевдослучайных последовательностей учитывается, что в системах безопасности они должны не только производить исходные последовательности, похожие на случайных, но и иметь свойство непредсказуемости. Это значит, что противник или злоумышленник по имеющимся разделам знаков выходной последовательности не может определить или предусмотреть неизвестные ему знаки с вероятностью большей, чем при случайном угадывании, владея реальными вычислительными и временными возможностями.

Генераторы, которые строятся на нелинейных регистрах сдвига с обратными связями, имеют преимущество перед другими генераторами в увеличении длины генерируемых последовательностей при одной и той же максимальной степени полинома. Класс нелинейных регистров сдвига значительно шире линейных. Графические тесты для исследования таких полиномов позволяют визуально исследовать генерируемые последовательности

Актуальность работы определяется практической потребностью промышленности, транспорта, связи и других областей в ИС, обладающих возможностями обнаружения нештатных режимов и отказов в реальном времени.

Целью работы является исследование полиномов для регистров сдвига с нелинейными обратными связями при помощи гистограмм.

В связи с этим разработана программная модель регистра сдвига с нелинейными связями, произведено моделирование его работы. Полученные результаты подтвердили работоспособность предложенной модели.