

## СЛОЖНОСТЬ РАСПОЗНАВАНИЯ СВОЙСТВ ФУНКЦИЙ ТРЕХЗНАЧНОЙ ЛОГИКИ, ПРЕДСТАВЛЕННЫХ ПОЛИНОМАМИ

*к.т.н., доцент НТУ "ХПИ" А.Н. Рысованый, Д.В. Зыков,  
С.А. Сильченко, И.И. Нежурина, НТУ ХПИ, г. Харьков*

В компьютерных системах регистры сдвига с обратными связями используются как непосредственно, так и в составе других устройств. В последнем случае качество операций генерации случайных последовательностей и хеширования определяется, в первую очередь, качеством используемых генераторов ПСП. Таким образом, именно от свойств генераторов ПСП, особенно в тех случаях, когда необходимо обеспечить устойчивую работу комбинационной схемы при наличии случайных и умышленных деструктивных воздействий, в значительной степени зависит надежность процессов сбора, обработки, хранения и передачи информации. К ним предъявляются жесткие требования, в первую очередь по таким параметрам, как непредсказуемость, статистические и периодические свойства. На основе таких регистров строятся и сигнатурные анализаторы (СА), которые применяются для тестового диагностирования цифровых объектов. При диагностировании некоторых классов цифровых схем (таких как программируемые логические матрицы) оказывается неэффективным псевдослучайный тест с линейного регистра сдвига с обратными связями, который связан с большим числом сходящихся разветвлений и специальным видом неисправностей в таких схемах. Кроме того, для контроля схем, которые имеют три стабильных состояния, а также линий передачи данных, имеющих три уровня сигнала, предпочтительнее использовать устройства, предназначенные именно для решения таких задач. В настоящее время не существует единых подходов к выбору полиномов для регистров сдвига с нелинейными обратными связями.

В работе исследуются свойства полиномов в поле  $GF(3)$  и их применение в компьютерных системах. Показано, что в отличие от линейных СА обратный полином по отношению к исследуемому не позволяет получить инверсную последовательность такой же длины. Установлено, что цикл генерации полиномов в поле  $GF(3)$  раскладывается ровно наполовину с инверсными значениями друг другу. Показано, что двукратные ошибки пропускаются нелинейным сигнатурным анализатором только тогда, когда длина входной последовательности превышает половину периода генерации образующего полинома. В этом случае число таких ошибок линейно зависит от длины исследуемой последовательности.