УДК 681.324:621.396

А.Н. Рысованый, В.В. Гоготов

Национальный технический университет «ХПИ», Харьков

АНАЛИЗ ЭФФЕКТИВНОСТИ МЕТОДИК ПОСТРОЕНИЯ НЕЛИНЕЙНОГО ГЕНЕРАТОРА ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ИСПОЛЬЗОВАНИЕМ БЛОКА СЛОЖЕНИЯ ПО МОДУЛЮ 3

В результате исследований проведено: анализ эффективности методик построения генератора псевдослучайных последовательностей с использованием блока сложения по модулю 3, который может применяться для тестирования аналогичных нелинейных схем; математическое описание функционирования генератора, на основании которого построен нелинейный генератор псевдослучайных последовательностей. В работе показано, что полнота не обнаружения неисправностей цифровой схемы в первую очередь зависит от качества тестовых воздействий.

Ключевые слова: *нелинейный регистр сдвига, полином, последовательность максимальной длины.*

Введение

Постановка проблемы. Классическая стратегия тестирования цифровых схем основана на формировании тестовых последовательностей, позволяющих обнаруживать заданные множества их неисправностей. При этом для проведения процедуры тестирования, как правило, хранятся как сами последовательности, так и эталонные выходные реакции схем на их воздействие. В процессе самой процедуры тестирования на основании сравнения выходных реакций с эталонными принимается решение о состоянии проверяемой схемы.

Для ряда выпускаемых в настоящее время схем классический подход требует временных затрат как на формирование тестовых последовательностей, так и на процедуру тестирования. Кроме того на проведение тестового эксперимента требуется наличие сложного оборудования. В связи с этим стоимость и время, необходимые для реализации классического подхода, растут быстрее, чем сложность цифровых схем, для которых он используется. Поэтому новые решения, позволяющие значительно упростить как процедуру построения генераторов тестовых последовательностей, так и проведение тестового эксперимента, являются актуальными.

Для реализации генератора тестовой последовательности используются алгоритмы, позволяющие избежать сложности их синтеза:

– формирование всевозможных тестовых наборов, то есть полного перебора двоичных комбинаций. В результате применения подобного алгоритма генерируются счётчиковые последовательности;

– формирование псевдослучайных тестовых последовательностей;

– формирование случайных тестовых наборов, с требуемыми вероятностями единичного и нулевого символов по каждому входу цифровой схемы.

Основным свойством рассмотренных алгоритмов формирования тестовых последовательностей является то, что в результате их применения воспроизводятся последовательности очень большой длины. Поэтому на выходах проверяемой цифровой схемы формируются её реакции, имеющие такую же длину. Естественно возникает проблема их запоминания, хранения и затрата на обработку этих последовательностей. Простейшим решением, позволяющим значительно сократить объём информации об эталонных выходных реакциях, является использование линий передачи данных, имеющих три уровня сигнала $(+, -, 0)$ с использованием устройств, предназначенных именно для решения таких задач.

Таким образом, возникает необходимость в анализе эффективности методик построения генератора псевдослучайных последовательностей с использованием блока сложения по модулю 3, который бы позволял генерировать последовательности максимальной длины.

Анализ литературы. В [1 – 8] рассмотрены свойства и особенности последовательностей максимальной длины, показан подход к построению генераторов псевдослучайных последовательностей.

Теория конечных полей рассмотрена в [1, 10].

В [11 – 16] рассмотрены принципы построения и применения сигнатурного анализа.

В [17, 18] автор утверждает, что актуальной научной задачей является развитие теории генераторов псевдослучайных последовательностей, в том числе создание новых алгоритмов генерации псевдослучайных последовательностей, сочетающих в себе непредсказуемость, высокое быстродействие и эффективную программную реализацию на различных платформах. Одним из направлений решения данной задачи является совершенствование алгоритмов формирования цифровых последовательностей, основанных на использовании сумматоров.

Основные свойства и структурные особенности последовательностей максимальной длины описаны в [20, 21].

Однако [9] «значительная часть установленных здесь фактов – не доказанные теоремы, а эмпирические наблюдения, ожидающие смелых исследователей».

Поэтому вопросы построения нелинейного генератора псевдослучайных последовательностей с использованием блока сложения по модулю 3 для линий передачи данных, имеющих три уровня сигнала, остается открытым, поскольку ответы на них позволяли бы находить полиномы с генерацией последовательности максимальной длины, также открытым остается вопрос анализа эффективности методик построения генератора псевдослучайных последовательностей.

Целью статьи является построение нелинейного генератора псевдослучайных последовательностей с использованием блока сложения по модулю 3 с анализом эффективности методик построения генератора псевдослучайных последовательностей.

Основная часть

Наиболее часто при формировании псевдослучайных последовательностей используются два метода. Первый из них лежащий в основе большинства программных датчиков псевдослучайных чисел, использует рекуррентные соотношения. Этот метод обладает рядом недостатков, в частности, малой периодичностью. Применительно к проблеме тестирования цифровых схем периодичность может заметно снизить полноту контроля. Кроме того, он отличается сложностью практической реализации.

Поэтому наиболее широко применяется второй метод, основанный на использовании соотношения

$$a_k = \sum_{i=1}^{m} \oplus \alpha_i a_{k-i},\ k = 0,1,2,\ldots,$$

где k – номер такта; $a_k \in \{0,1,2\}$ – символы последовательности; $\alpha_i \in \{0,1,2\}$ – постоянные коэффициенты; $\sum_{i=1}^{m} \oplus$ – операция суммирования по модулю три m логических переменных. При соответствующем выборе коэффициентов α_i на основании характеристического полинома:

$$\varphi(x) = 1 \oplus a_1 x^1 \oplus a_2 x^2 \oplus \ldots \oplus a_{m-1} x^{m-1} \oplus a_m x^m,$$

который должен быть примитивным, иметь последовательность максимальной длины, равную $3^m - 1$.

По приходу каждого синхронизирующего импульса в первый разряд регистра сдвига записывается информация, соответствующая выражению:

$$a_1(K) = y(K) \oplus \sum_{i=1}^{m} \oplus \alpha_i a_i(K-1),$$

где $y(K) \in \{0,1,2\}$ – k-й символ сжимаемой последовательности $\{y(K)\}$, $K = \overline{1,l}$; $\alpha_i \in \{0,1,2\}$ – коэффициенты порождающего полинома $\varphi(x)$; $a_1(k-1) \in \{0,1,2\}$ – содержимое *i*-го элемента памяти регистра сдвига 1 в (k – 1) такт. Процедура сдвига информации в регистре описывается соотношением

$$a_j(k) = a_{j-1}(k-1),\ j = \overline{2,m}.$$

Таким образом, полное математическое описание функционирования генератора имеет следующий вид:

$$a_i(0) = 0;\ i = \overline{1,m};\ a_1(k) = y(k) \oplus \sum_{i=1}^{m} \oplus \alpha_i a_i(k-1);$$

$$a_j(k) = a_{j-1}(k-1),\ j = \overline{2,m},\ k = \overline{1,l},$$

причём *l*, как правило, принимается равным или меньше величины $(3^m - 1)$, и соответственно является длиной сжимаемой последовательности.

По истечении *l* тактов функционирования сигнатурного анализатора на его элементах памяти фиксируется код, который представляет собой сигнатуру.

Для того чтобы обеспечить различные режимы испытаний, генераторы испытуемых сигналов должны удовлетворять ряду требований (многоканальность, быстродействие, достаточная длина периода и т.д.). В основе наиболее перспективного метода построения быстродействующего параллельного генератора псевдослучайных последовательностей испытательных сигналов лежит идея использования (в качестве независимых последовательностей для формирования разрядов очередного кода) участков одной и той же последовательности. В данном случае генерирование различных участков осуществляется с помощью η-входовых сумматоров по модулю три, т.е. $\eta \in \{3,m\}$, где m – разрядность регистра сдвига. Соединения сумматоров по модулю три с разрядами регистра сдвига определяются набором коэффициентов $\delta_i(1) \in \{0,1,2\}$ (i = 1, 2, ... , m), значения которых зависят от величины сдвига *l* (*l* = 1, 2, 3, …) и вида порождающего полинома (рис. 1).

Методика выбора коэффициентов $\delta_i(1)$, однозначно определяющих связи многовходового сумматора по модулю три, описывается на итерационном подходе, когда на основании $\delta_i(h)$, по расчётным соединениям находятся $\delta_i(1)(h = 1, 2, \ldots, h < l)$.

Предположим, что коэффициенты $\delta_i(1)$ и $\delta_i(S)$, позволяющие получить сдвинутые копии последовательности на 1 и S тактов, известны; тогда содержимое $a_1(k + 1)$ первого разряда регистра сдвига в (k + 1)-м такте работы определяется следующим образом:

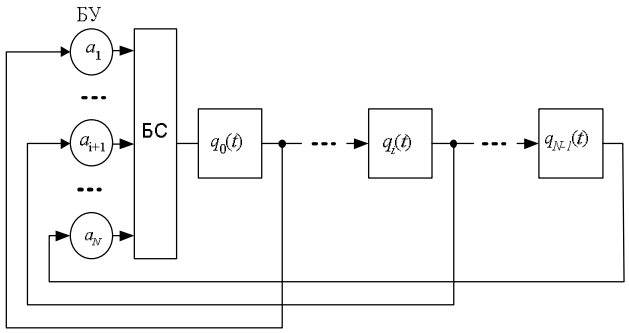

Рис. 1. Схема генератора при k = 1

$$a_1(k+1) = \sum_{i=1}^{m} \oplus \delta_i(1) a_i(k);\ \ k = 0,1,2...$$

где $a_i(k)$ – содержимое i-го разряда регистра сдвига в к-м такте его работы, а символ $\sum \oplus$ означает операцию суммирования по модулю три. Содержимое первого разряда регистра сдвига в (k + s)-м такте работы имеет вид

$$a_1(k+s) = \sum_{i=1}^{m} \oplus \delta_i(s) a_i(k)$$

для определения содержимого первого разряда регистра сдвига в (k + 1 + s)-м такте необходимо предварительно выбрать численное значение коэффициентов $\delta_i(1+s)$.

С другой стороны, $a_1(k + 1 + s)$ можно найти следующим образом:

$$a_1(k+1+s) = \sum_{i=1}^{m} \oplus \delta_i(s) a_i(k+1),$$

где $a_i(k+1)$ принимает вид

$$a_1(k+1) = \sum_{i=1}^{m} \oplus \delta_i(1) a_i(1);$$

$$a_{1+p}(k+1) = \sum_{n=1}^{m-p} \oplus \delta_n(1) a_{n+p}(k) \oplus$$

$$\oplus \sum_{n=1}^{p} \oplus \delta_{m-p+n}(1) a_m(k-n)(p = 1, m-1).$$

Возникает проблема анализа эффективности разрабатываемой методики построения нелинейного генератора псевдослучайных последовательностей с использованием блока сложения по модулю 3.

Полнота не обнаружения неисправностей цифровой схемы в первую очередь зависит от качества тестовых воздействий. Если определённая неисправность не проявляется в виде искажения их символов, то она не может быть обнаружена в результате применения сигнатурного анализа, который является не более чем эффективным методом сжатия потока данных. Поэтому если этот поток не несёт информации о неисправности, то она и не появится после его сжатия.

Для оценки этой характеристики могут использоваться разные подходы и методы. Наиболее широко применяемым является вероятностный подход, сущность которого заключается в определении вероятности P_n не обнаружения ошибок в анализируемой последовательности данных. Причём в рассматриваемом случае оценивается вероятность, зависящая только от метода сжатия, и не учитываются другие факторы.

Величина P_n рассчитывается для достаточно общего случая, приближённо соответствующего реальным примерам. Предполагается, что эталонная последовательность данных может равновероятно принимать разное значение, а любая конфигурация ошибочных бит может быть равновероятным событием.

Далее, использую алгоритм деления полиномов как математический аппарат формирования сигнатуры, показываем, что для *l*-разрядного делимого вычисляются *l*-m-разрядное частное и m-разрядный остаток (сигнатура). При этом соответствие реальной последовательности, состоящей из *l* бит, эталонной оценивается только по равенству их m - разрядных сигнатур. Для $3^{l\text{-}m}$ различных частных будет формироваться одинаковая сигнатура. Это свидетельствует о том, что $3^{l\text{-}m}-1$ ошибочных *l*-разрядных последовательностей будут считаться соответствующими одной – эталонной. Учитывая равновероятность ошибочных последовательностей данных, можно заключить, что $3^{l\text{-}m} - 1$ ошибочных последовательностей, инициирующих эталонную сигнатуру, не обнаруживаемы. Таким образом, вероятность P_n необнаружения ошибок в анализируемой последовательности данных будет вычисляться как отношение:

$$P_n = (3^{l-m} - 1) / (3^l - 1),$$

где $3^l - 1$ равняется общему числу ошибочных последовательностей.

Выражение для условия *l*>>m преобразуется к более простому виду:

$$P_n = 1 / 3^m,$$

которое может служить основным аргументом для обоснования высокой эффективности сигнатурного анализа.

Выводы

В результате исследований проведено: анализ эффективности методик построения генератора псевдослучайных последовательностей с использованием блока сложения по модулю 3, который может применяться для тестирования аналогичных нелинейных схем; математическое описание функционирования генератора, но основании которого построен нелинейный генератор псевдослучайных последовательностей. В работе показано, что полно-

та не обнаружения неисправностей цифровой схемы в первую очередь зависит от качества тестовых воздействий.

Список литературы

1. Иванов М.А., Чугунков И.В. Теория, применение и оценка генераторов псевдослучайных последовательностей. – М.: КУДИЦ-ОБРАЗ, 2003. – 240 с.

2. Теория и применение псевдослучайных сигналов / А.И. Алексеев, А.Г. Шереметьев, Г.И. Тузов, В.И. Глазов. – М.: Наука, 1969. – 240 с.

3. Доценко В.И., Фараджаев Р.Г. Анализ и свойства псевдослучайных последовательностей максимальной длины // Автоматика и телемеханика. – 1969. – № 11. – С. 119-127.

4. Доценко В.И., Фараджаев Р.Г., Чхартишвили Г.С. Свойство последовательностей максимальной длины с Р-уровнями // Автоматика и телемеханика. – 1971. – № 8. – С. 189-194.

5. Макушльямс Ф. Дж., Слоан Н. Дж. А. Псевдослучайные последовательности и таблицы // ТИИЭР. – 1976. – № 12. – С. 80-95.

6. Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. – М.: Мир, 1976. – 376 с.

7. Блейхут Р. Теория и практика кодов, контролирующих ошибки. – М.: Мир, 1986. – 576 с.

8. Элспас Б. Теория автономных линейных последовательных сетей // Кибернетический сборник. – 1963. – Вып. 7. – С. 90-128.

9. Арнольд В.И. Динамика и статика полей Галуа: Курс лекций. – М.: Мехмат МГУ. – 2004. – [электронный ресурс]: http://ftp.mccme.ru.

10. Зензин О.С., Иванов М.А. Стандарт криптографической защиты XXI века – AES. Теория конечных полей / Под ред. М.А. Иванова. – М.: КУДИЦ-ОБРАЗ, 2002. – 340 с.

11. Пухальский Г.И., Новосельцева Т.Я. Цифровые устройства: Учебное пособие для втузов. – С.-Пб.: Политехника, 1996. – 126 с.

12. Основы сигнатурного анализа ЭВМ и вычислительных систем: Учебное пособие / А.Н. Рысованый и др. – Х.: ХВУ, 1996. – 42 с.

13. Основи теорії синтезу сигнатурних аналізаторів. Навчальний посібник / За ред. О.М. Рисованого. – Х.: ХВУ, 1998. – 122 с.

14. Латыпов Р.Х. Воспроизведение тестовых наборов и сжатие данных нелинейными регистрами сдвига // Автоматика и телемеханика. – М.: Наука. – 1989. – № 10. – С. 167-172.

15. Барашко А. С. Характеристическая функция нелинейного сигнатурного анализатора // Электронное моделирование. – 2000. – Т. 22, № 6. – С. 59-65.

16. Науменко М.І., Стасєв Ю.В., Кузнєцов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів: Монографія. – Х.: ХУ ПС, 2005. – 267 с.

17. Тан Найнг Со, Тун Мья Аунг, Иванов М.А. Генераторы псевдослучайных последовательностей в задачах защиты информации // Научная сессия МИФИ, 2006. Сб. научн. тр. – М.: МИФИ. – 2006. – № 12. – С. 115-116.

18. Тун Мья Аунг. Генераторы псевдослучайных последовательностей, основанные на использовании регистров сдвига со стохастическими обратными связями // Научная сессия МИФИ, 2007. Сб. научн. тр. – М.: МИФИ. – 2007. – № 12. – С. 137-138.

19. Рысованый А.Н., Гоготов В.В. Выбор полиномов для нелинейных регистров сдвига с обратными связями по критерию формирования последовательности максимальной длины // Системи управління, навігації та зв'язку. – К.: Центральний науково-дослідний інститут навігації і управління. – 2007. – Вип. 1.– С. 77-79.

20. Arvillias A.C., Maritsas D.G. Toggle-Registers Generating in Parallel k kth Decimaitions of m-Sequences $x^p + x^k + 1$ Design Tables // IEEE Transaction on Computers. V. C-28. – 1979. – № 2. – P. 89-100.

21. Pradhan D.K., Hsiao M.Y., Patel A.M., Su S.Y. Shift Registers Designed for on-line Fault Detection // Proceedings of 8^{th} International Conference on Fault-Tolerant Computing. – 1978. – P. 173-178.

Поступила в редколлегию 22.08.2008

Рецензент: д-р техн. наук, проф. И.И. Обод, Национальный технический университет «ХПИ», Харьков.

АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДИК ПОБУДОВИ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ З ВИКОРИСТАННЯМ БЛОКУ СКЛАДАННЯ ПО МОДУЛЮ 3

О.М. Рисований, В.В. Гоготов

В результаті досліджень проведено: аналіз ефективності методик побудови генератора псевдовипадкових послідовностей з використанням блоку складання за модулем 3, який може застосовуватися для тестування аналогічних нелінійних схем; математичний опис функціонування генератора, на підставі якого побудований нелінійний генератор псевдовипадкових послідовностей. У роботі показано, що повнота не виявлення несправностей цифрової схеми в першу чергу залежить від якості тестових послідовностей.

Ключові слова: *нелінійний регістр зсуву, полином, послідовність максимальної довжини.*

ANALYSIS OF METHODS' EFFICIENCY OF GENERATOR CONSTRUCTION OF PSEUDORANDOM SEQUENCES WITH THE USE OF ADDITION BLOCK ON THE MODULE 3

A.N. Risovaniy, V.V. Gogotov

It is conducted as a result of researches: analysis of efficiency of methods of construction of generator of pseudocasual sequences with the use of block of addition on the module 3, which can be used for testing of analogical nonlinear charts; mathematical description of functioning of generator, but foundation of which the nonlinear generator of pseudocasual sequences is built. It is shown in work, that plenitude of not finding out the disrepairs of digital chart above all things depends on quality of test influences.

Keywords: *nonlinear shift register, polynomial, sequence of maximal length.*