УДК 681.324.067

А.А. ТОРБА, канд. техн. наук, В.А. БОБУХ, С.Г. ЕЛАКОВ, А.З. СТЕПЧЕНКО

ПОВЫШЕНИЕ БЫСТРОДЕЙСТВИЯ ГЕНЕРАТОРОВ СЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ФИЗИЧЕСКИХ ДАТЧИКОВ

Ключевой проблемой технических средств защиты информации является генерация случайных равновероятных последовательностей на основе физических датчиков. Важным параметром таких генераторов является быстродействие, измеряемое количеством генерируемых случайных битов в секунду (бит/с).

Рассмотренные в статье [1] методы генерации случайных последовательностей на основе физических датчиков шума обладают ограниченным быстродействием, потому что скорость генерации случайных битов, определяемая частотой заполнения сдвигающего регистра **Fo** (см. рис.1), должна быть в 3...5 раз меньше средней частоты шумовых импульсов **Fш** на выходе датчика. Повышение быстродействия возможно за счет применения более широкополосных квантовых генераторов шума. Однако это значительно удорожает генератор, а также приводит к увеличению его габаритов и веса.

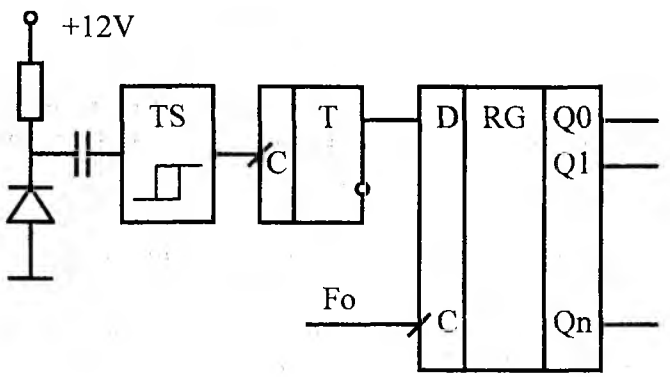

Рис. 1

Если нарушить приведенное в статье [1] ограничение, то есть увеличить частоту заполнения сдвигающего регистра **Fo** в несколько раз, то это приведет к ухудшению статистических свойств генерируемой случайной последовательности. Экспериментально проверено, что нарушение указанных ограничений приводит к увеличению количества серий из двух и трех последовательных нулей и единиц.

В той же статье [1] приведены и методы улучшения статистических свойств генерируемых случайных двоичных последовательностей, в частности, метод «дельта квадрат», то есть объединение элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» двух генерируемых битов. На рис. 2 приведена функциональная схема генератора, в которой схемой «ИСКЛЮЧАЮЩЕЕ ИЛИ» объединены: генерируемый шумовым датчиком случайный бит и другой бит, сгенерированный ранее. Для того, чтобы эти биты были независимы, необходимо выбирать длину (m) сдвигающего регистра в два-три раза больше, чем разрядность (n) случайных слов, считываемых в компьютер.

Эту схему (рис. 2) можно рассматривать и как сдвигающий регистр, замкнутый в кольцо (кольцевой счетчик), у которого элемент «ИСКЛЮЧАЮЩЕЕ ИЛИ» используется для инверсии в случайные равновероятные моменты времени сигнала обратной связи. Известно, что у обычного кольцевого счетчика последовательности будут повторяться с периодичностью, не превышающей длину (m) этого счетчика. Поэтому разрядность (длину) регистра желательно увеличивать.

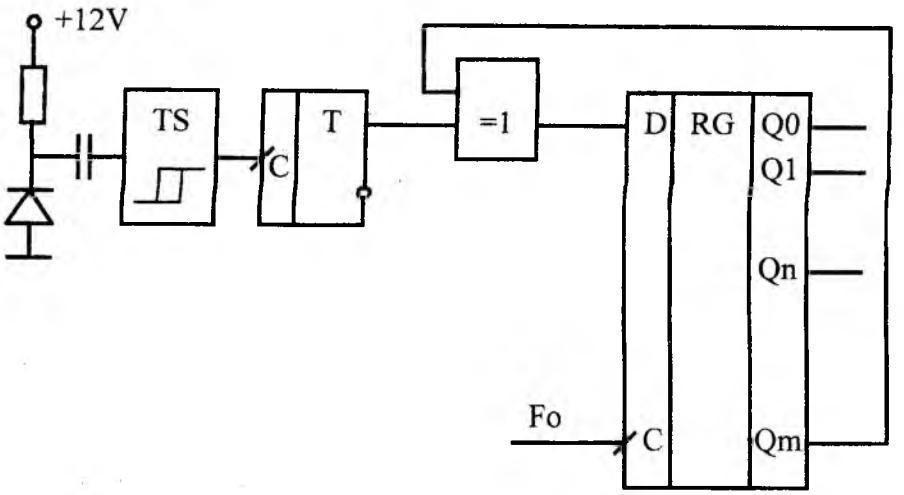

Рис. 2

Но можно значительно увеличить периодичность сдвигающего регистра [2], если реализовать обратную связь с дополнительным элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» (см. рис. 3). Максимальная периодичность такого линейного рекуррентного регистра (ЛРР) равна:

$$K = 2^m - 1$$

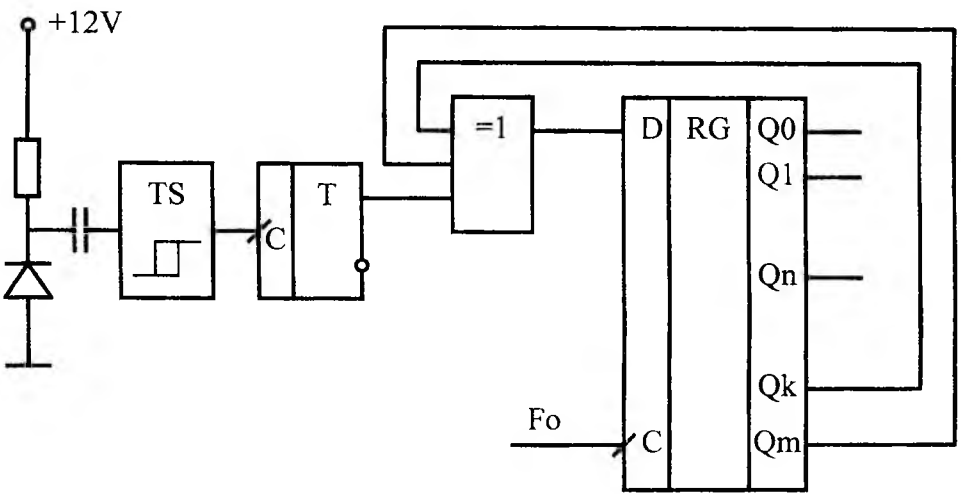

Рис. 3

Так, 60-ти разрядный регистр при тактовой частоте 10 МГц имеет период повторения несколько миллионов лет. А 100-разрядный регистр имеет период повторения 10^{18} лет, то есть в миллион раз превышающий возраст Вселенной.

Известно, что ЛРР является идеальным генератором *псевдослучайных равновероятных последовательностей*. Каждый отрезок такой последовательности можно рассматривать как *случайный*, если не известна предыстория его формирования. Для этого необходимо, чтобы каждое слово этой последовательности считывалось в случайные моменты времени и длина каждой считываемой последовательности была значительно меньше, чем пропущенное количество битов между считываниями.

Схему на рис. 3 можно рассматривать как сдвигающий регистр, в который вводятся случайные биты от источника с физическим датчиком шума, а цепь обратной связи с элементом

«ИСКЛЮЧАЮЩЕЕ ИЛИ» используется для улучшения статистических свойств случайной последовательности по методу «дельта квадрат».

Эту же схему (рис. 3) можно рассматривать как генератор псевдослучайных последовательностей на основе ЛРР, в котором в случайные равновероятные моменты времени «разрушается рекуррента» за счет инверсии сигнала обратной связи элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ», что делает такие последовательности непредсказуемыми, то есть случайными.

Какой из этих подходов преобладает, определяется отношением частоты сдвига **Fo** к средней частоте шума физического датчика **Fш**. Если частота шумового датчика **Fш** соизмерима или больше, чем тактовая частота сдвигающего регистра **Fo**, то схему на рис. 3 необходимо рассматривать, как обычный генератор случайных сигналов с улучшенными параметрами по методу «дельта квадрат». Если частота **Fo** значительно превышает среднюю частоту датчика шума **Fш** (в 100 и более раз), то эту схему необходимо рассматривать, как генератор на основе ЛРР с «разрушением рекурренты» в равновероятные случайные моменты времени. Причем, если длина рекурренты превышает *миллионы лет*, а разрушается она *миллионы раз в секунду*, то говорить о возможности восстановления ее предыстории бессмысленно.

Для повышения надежности генератора случайных равновероятных последовательностей, а также для повышения устойчивости генерируемых случайных последовательностей к алгоритмам криптоанализа предлагается *многоканальная схема* с горячим резервированием каналов физических датчиков шума (на рис. 4 приведена двухканальная схема).

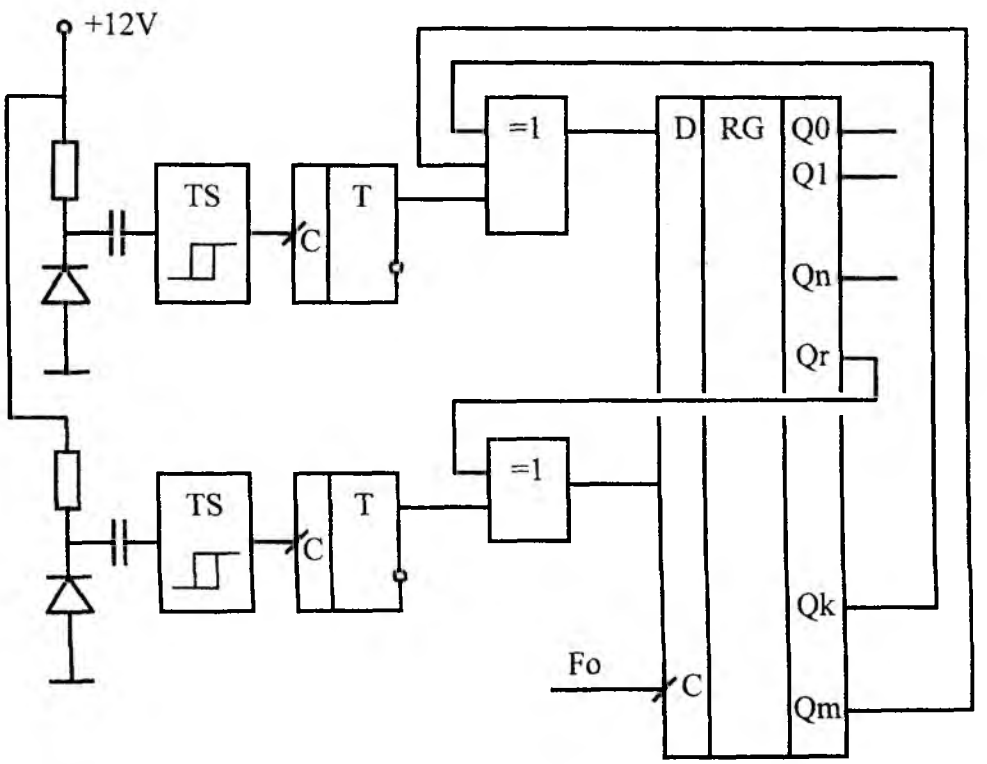

Рис. 4

Эта схема позволяет многократно «разрушать рекурренту» при прохождении случайного сигнала по сдвигающему регистру, что делает генерируемые последовательности еще более непредсказуемыми и затрудняет их криптоанализ. Это позволяет также повысить скорость генерации случайных последовательностей, то есть увеличить частоту **Fo** по сравнению с частотой **Fш** для каждого физического датчика.

Случайный характер сигнала сохраняется даже при неработоспособности всех каналов физических датчиков шума, кроме одного. Этим достигается горячее резервирование.

На основе вышеизложенного сформулируем требования к генераторам случайных последовательностей на основе физических датчиков шума с высоким быстродействием (на примере схемы на рис.4):

1. Длина сдвигающего регистра (m) должна значительно превышать разрядность (n) считываемых в компьютер случайных слов. Это позволяет также реализовать период рекурренты в несколько миллионов лет и более.
2. Количество пропущенных случайных битов между соседними операциями считывания должно значительно превышать разрядность считываемых слов.
3. Случайные временные интервалы между операциями считывания определяются спецификой работы компьютера, например, за счет многозадачной работы операционной системы.
4. Многоканальные схемы датчиков физического шума позволяют повысить надежность системы и затрудняют криптоанализ генерируемых случайных последовательностей.

Авторами реализованы генераторы случайных последовательностей со скоростью генерации от 5 до 15 Мбит/с. Максимальные скорости определяются быстродействием примененной элементной базы и скоростью ввода информации в компьютер через слот PCI-32/33МГц. Использовалась двухканальная схема резервирования физических датчиков шума. Результаты тестирования подтвердили правильность принятых решений.

Список литературы: 1. *А.А. Торба, С.Г. Елаков, А.З. Степченко* Генерация равновероятных случайных последовательностей на основе физических датчиков // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119. С.108-113. 2. Деклар. пат. 36108 України, МКІ 6 G06F7/58, G07C15/00. Спосіб генерації випадкових чисел та пристрій для його здійснення/ О.О. Торба (Україна). – 4 с. іл.; Опубл. 16.04.2001, Бюл. № 3.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 23.04.2002