УДК 681.324.067

А. А. ТОРБА, канд. техн. наук, В. А. БОБУХ, канд. техн. наук, А. А. ТОРБА

АППАРАТНЫЕ ГЕНЕРАТОРЫ КВАЗИСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Постановка задачи экспериментальных исследований

Известны физические ограничения на увеличение скорости формирования квазислучайных последовательностей, которые определяются частотой *F*ш случайных шумовых импульсов на выходе датчиков шума (Noise Source – NS). Повышение быстродействия аппаратных генераторов квазислучайных последовательностей (АГКСП) сопровождается ухудшением статистических параметров формируемых квазислучайных битов, а именно, ухудшается свойство независимости соседних битов (это свойство проверяется автокорреляционным тестом, блочным тестом Покера, тестом серий и др.)

Экспериментально установлено, что максимальная частота *Fo* формирования квазислучайных последовательностей должна быть в 5÷8 раз меньше частоты *F*ш случайных импульсов на выходе физического датчика шума [1]. Т.е. для шумовых диодов КГ401 с частотой шумовых импульсов *F*ш = 2÷10 *МГц* скорость формирования квазислучайных последовательностей не может превышать 1 *Мбит/с*.

Цель проведенных экспериментальных исследований – разработка методов повышения скорости формирования квазислучайных последовательностей без ухудшения их статистических параметров.

Метод объединения нескольких статистически независимых потоков

Известен метод горячего резервирования статистически независимых физических датчиков шума с объединением выходных сигналов каждого канала элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» [2]. В результате экспериментальных исследований установлено, что этот метод позволяет увеличить быстродействие аппаратных генераторов пропорционально количеству датчиков шума.

Последовательность формируемых квазислучайных битов может рассматриваться как поток, у которого между битами, разнесенными во времени на значительные расстояния, отсутствуют статистические связи. Было предложено сдвигать во времени квазислучайные биты многоразрядными сдвигающими регистрами.

Объединение элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» разнесенных во времени статистически независимых квазислучайных битов от одного датчика шума можно рассматривать как объединение нескольких статистически независимых случайных потоков. Предложен метод повышения быстродействия аппаратных генераторов квазислучайных битов с объединением отводов многоразрядного сдвигающего регистра элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» (см. рис. 1) [3].

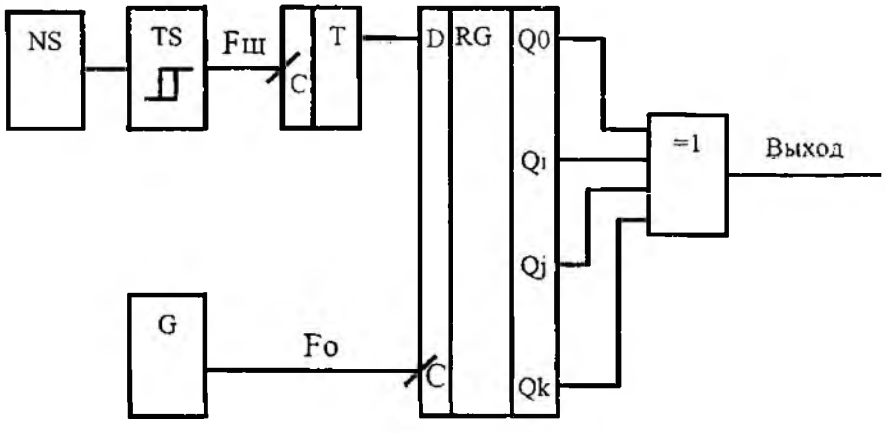

Рис. 1

На рис. 2 приведены результаты измерений зависимости нормированных коэффициентов автокорреляционных функций с единичной задержкой $K(1)$ от скорости формирования квазислучайных битов Fо для исходной схемы (n=1) и для схем с объединением элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» статистически независимых потоков от нескольких отводов сдвигающего регистра (n=2, n=3, n=4).

По горизонтальной оси отложено отношение частоты импульсов на выходе шумового диода Fш (фиксированная константа) к частоте формирования квазислучайных битов Fо (изменяемый аргумент).

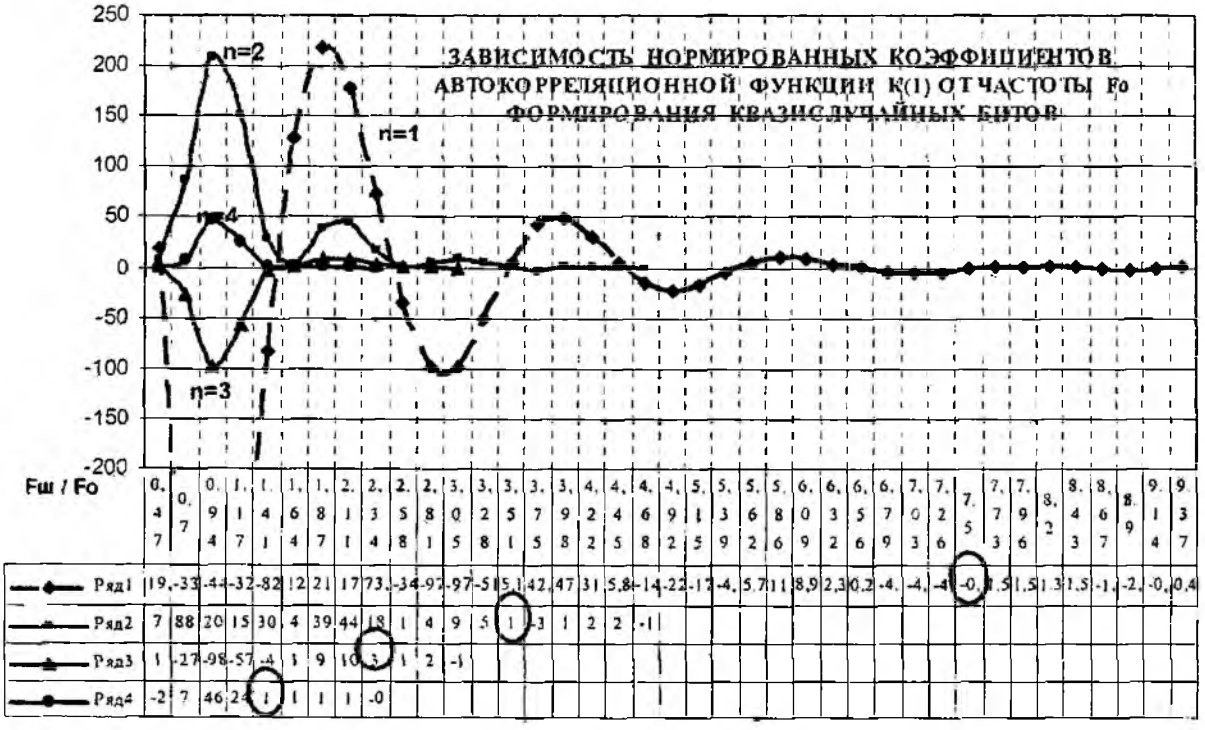

Рис. 2

Для исходной схемы без отводов (n=1) только при отношении Fш/Fо = 7,5 значения коэффициентов нормированной автокорреляционной функции $K(1)$ попадают в интервал $\pm 3\sigma$, т.е. соседние биты становятся статистически независимыми.

Для схемы с объединением элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» двух отводов сдвигающего регистра (n=2) коэффициенты автокорреляционной функции попадают в интервал $\pm 3\sigma$ при отношении Fш/Fо = 3,5 (см. рис. 2), т.е. скорость формирования квазислучайных битов увеличивается в два раза.

Для расчета коэффициента увеличения скорости формироваиия k определяют максимальную частоту Fо формирования квазислучайных последовательностей для исходной схемы, т.е. частоту, при которой формируемые квазислучайные биты проходят все статистические тесты. Аналогично определяют максимальную частоту Fо для схемы с объединением элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» нескольких потоков. Отношение этих частот численно равно коэффициенту увеличения скорости k аппаратного генератора квазислучайных последовательностей (АГКСП).

В результате экспериментов было подтверждено, что такое объединение не только увеличивает скорость формирования пропорционально количеству объединенных потоков, но и улучшает такой важный статистический параметр, как разность вероятностей генерируемых квазислучайных битов в соответствии с методом «Дельта-квадрат» [4].

Для увеличения скорости формирования квазислучайных битов в 20-30 раз необходимо применять очень длинные сдвигающие регистры (500 и более разрядов) с количеством отводов 20-30. Это приводит к неоправданно большим экономическим затратам.

Метод объединения случайных потоков с перестановками битов

На основе анализа схем аппаратных генераторов квазислучайных последовательностей (АГКСП) предложено подавать на элемент «ИСКЛЮЧАЮЩЕЕ ИЛИ» не случайные биты, следующие друг за другом, а разнесенные во времени биты за счет перестановок при помощи мультиплексора MS1 (см. рис. 3). На адресные входы мультиплексора MS1 подаются выходные сигналы дополнительного двоичного счетчика CT.

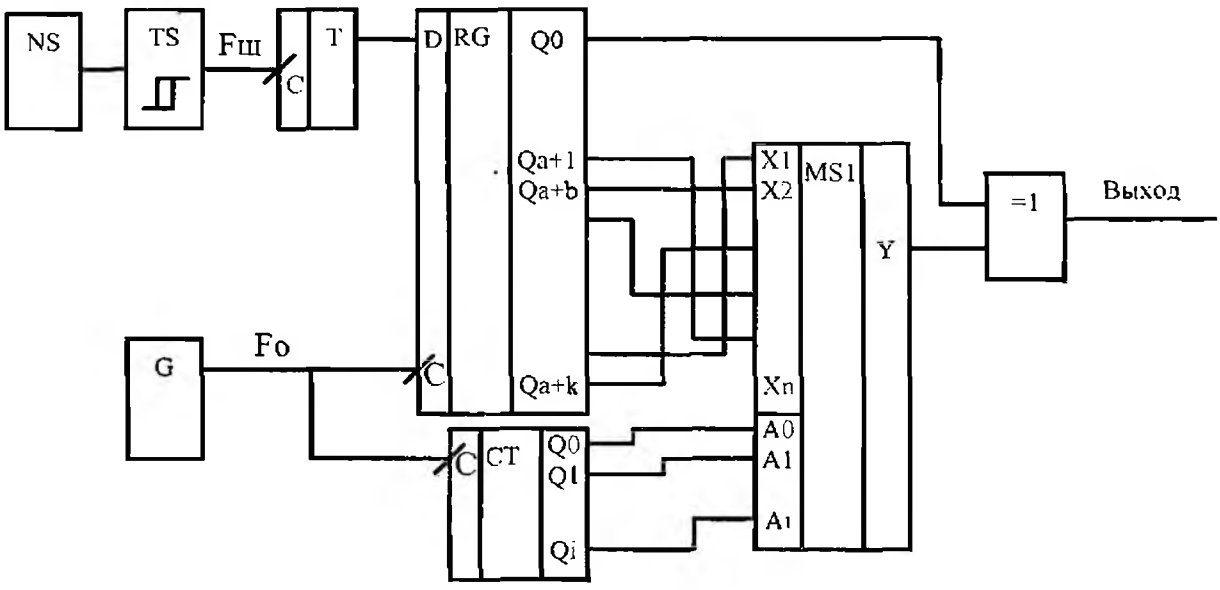

Рис. 3

Такие перестановки разносят во времени соседние биты (которые имеют значительные корреляционные связи) и тем самым уменьшают коэффициенты автокорреляционной функции с малыми задержками – $K(1)$, $K(2)$, но увеличивают коэффициенты для больших задержек (см. рис. 4).

Объединение сигналов с первого выхода Q0 регистра RG (исходная схема без перестановок) и выхода мультиплексора MS1 элементом «ИСКЛЮЧАЮЩЕЕ ИЛИ» позволяет значительно уменьшить результирующие коэффициенты автокорреляционной функции (см. рис. 4) и тем самым повысить быстродействие аппаратного генератора в $k = 4–7$ раз.

Проведение экспериментов с различными перестановками битов удалось значительно уменьшить коэффициенты автокорреляционных функций для сигналов на выходе мультиплексора с задержками от 1 до 6 (см. рис. 4) и тем самым увеличить скорость формирования квазислучайных битов примерно в 7 раз.

Многочисленные эксперименты с различными перестановками позволили сделать вывод о том, что максимальный коэффициент увеличения скорости формирования (k) аппаратного генератора квазислучайных последовательностей для мультиплексора с восьмью входами не может быть больше семи ($k \leq 7$).

Дальнейшее увеличение скорости формирования квазислучайных последовательностей возможно за счет применения мультиплексоров с 16-ю входами или применения каскадирования схем с перестановками.

Применение мультиплексоров с 16-ю входами позволит увеличить скорость формирования примерно в $k = 15$ раз, но при этом значительно увеличивается длина сдвигающего регистра.

Для реализации схем каскадирования сигнал с выхода элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» (см. рис. 3) подается на вход второго дополнительного сдвигающего регистра с отводами и со вторым дополнительным мультиплексором. Дополнительный элемент «ИСКЛЮЧАЮЩЕЕ ИЛИ» объединяет сигналы с выхода первого элемента «ИСКЛЮЧАЮЩЕЕ

ИЛИ» (т.е. с выхода первого каскада) и с выхода второго мультиплексора (т.е. с выхода второго каскада). Выход второго элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» является выходом схемы.

Рис. 4

До начала экспериментов с каскадированием ожидалось, что результирующее увеличение скорости формирования может достигать: $k = 7 * 7 = 49$ раз.

Но при одинаковых перестановках в двух каскадах результирующий коэффициент увеличения скорости формирования оказался равен коэффициенту для первого каскада, т.е. введение второго каскада не увеличивает результирующее быстродействие.

При экспериментах с различными перестановками в двух каскадах удалось поднять результирующий коэффициент увеличения скорости формирования до величины $k = 20 \div 25$. т.е. второй каскад увеличивает быстродействие только в 3÷3,5 раза.

Метод объединения потоков со случайными перестановками битов

Следующая группа экспериментов проводилась со случайными перестановками в одном каскаде (см. рис. 5). На адресные входы мультиплексора MS1 подавались случайные биты с дополнительного генератора квазислучайных последовательностей GR, реализованного на основе линейного рекуррентного регистра (ЛЛР) с разрушением рекурренты от датчика квазислучайных битов [5].

Расстояние между отводами сдвигающего регистра – b (см. рис. 5) желательно выбирать не менее четырех, потому что при случайных перестановках существует вероятность повторения одного и того же бита при следующих считываниях с выхода мультиплексора.

На рис. 6 приведены автокорреляционные функции для сигналов с выхода мультиплексора MS1 при расстояниях между отводами сдвигающего регистра $b = 5$. Сигналы на выходе мультиплексора имеют значительные корреляционные связи для задержек, кратных расстоянию между отводами сдвигающего регистра – b: 5, 10, 15, 20…

Применение схем со случайными перестановками позволяет увеличить скорость формирования битов на выходе элемента «ИСКЛЮЧАЮЩЕЕ ИЛИ» в $k = 3 \div 4$ раза.

Дальнейшее повышение быстродействия для схемы со случайными перестановками возможно за счет увеличения расстояния b между отводами (см. рис. 5). Но это приведет к значительному увеличению длины сдвигающего регистра RG.

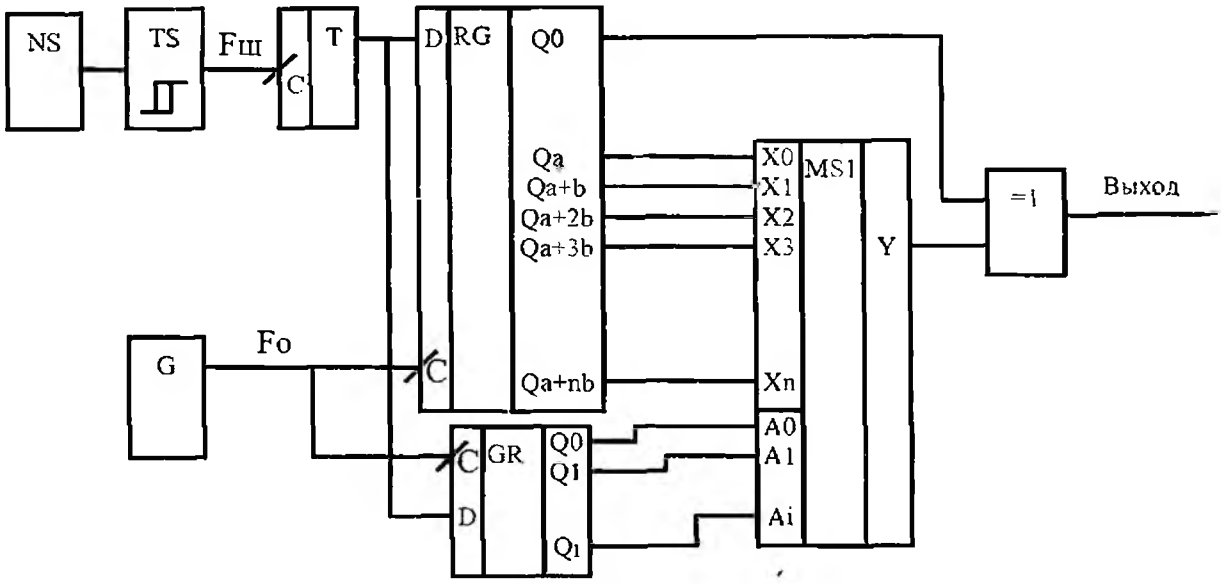

Рис. 5

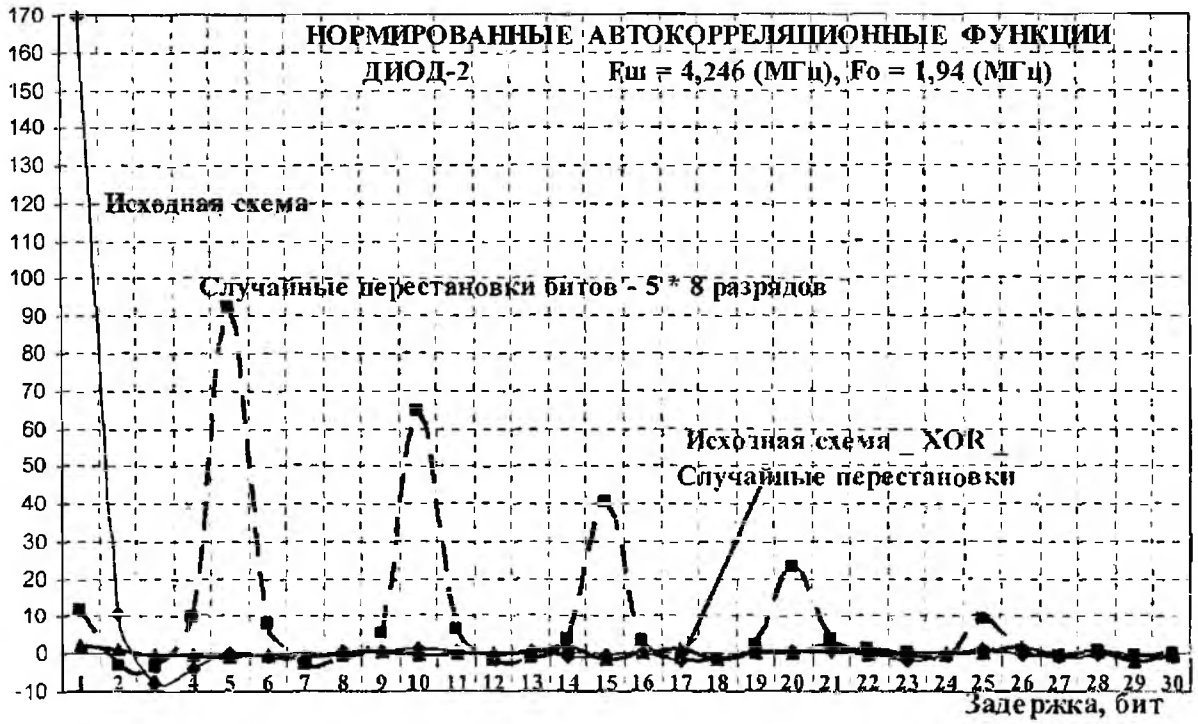

Рис. 6

Поэтому были проведены эксперименты по каскадированию схемы со случайными перестановками в первом каскаде и с детерминированными перестановками во втором каскаде (рис. 6).

Результирующий коэффициент увеличения скорости формирования для двухкаскадной схемы (с отводами через $b = 4$ *бита* в первом каскаде) составил $k = 60 \div 70$ раз.

Для двухкаскадной схемы (с отводами через $b = 5$ *бит* в первом каскаде) результирующий коэффициент увеличения быстродействия – не менее 100 раз.

Можно ещё увеличить коэффициент k до нескольких сотен за счет применения трехкаскадных или более «каскадных» схем.

Экспериментально проверено, что в схеме с шумовым диодом КГ401А, у которого Fш = 2,8 *МГц*, и коэффициенте увеличения скорости формирования $k = 100$ раз аппаратный

генератор формирует квазислучайные биты, которые проходят все статистические тесты на частоте $Fo = 33$ *МГц*.

Большинство шумовых диодов КГ 401А имеют частоту шумовых импульсов Fш не менее $5 \div 6$ *МГц*. Поэтому генератор с таким диодом будет проходить все статистические тесты при скорости формирования квазислучайных битов $Fo = 60$ *МГц*. А в схеме с горячим резервированием [2] частота формирования квазислучайных битов может быть не менее 100 *МГц*.

Оптимизация многокаскадных схем аппаратных генераторов квазислучайных последовательностей (АГКСП) с перестановками битов осуществляется по экономическому критерию – минимальное количество триггерных ячеек в применяемых программируемых логических интегральных схемах (ПЛИС).

Для построения двухкаскадной схемы АГКСП с коэффициентом увеличения скорости формирования $k \geq 100$ необходима ПЛИС с количеством триггерных ячеек не менее $180 \div 200$.

На ПЛИСах с количеством триггеров 128 возможно реализовать схему с коэффициентом увеличения быстродействия $k = 30 \div 40$.

Выводы

Объединение нескольких потоков квазислучайных битов позволяет увеличить скорость формирования АГКСП пропорционально количеству объединяемых потоков.

Для реализации коэффициента увеличения скорости формирования $k \geq 10$ необходимы сдвигающие регистры с очень большим количеством триггерных ячеек. Это приводит к неоправданно большим экономическим затратам.

Впервые предложенный метод повышения быстродействия АГКСП на основе перестановок битов в одном каскаде позволяет реализовать коэффициент увеличения быстродействия $k = 7 \div 15$ со значительно меньшим количеством триггерных ячеек.

Впервые предложенные методы повышения быстродействия на основе многокаскадных схем со случайными и детерминированными перестановками битов позволяют значительно увеличить быстродействие ($k \geq 100$) с оптимальным количеством триггерных ячеек.

Предложенные методы, кроме многократного увеличения быстродействия, позволяют также улучшить важный статистический параметр – разность вероятностей формируемых квазислучайных битов (на основе метода «Дельта-квадрат») в несколько десятков раз.

Список литературы: 1. *Торба А.А*, *Бобух В.А.*, *Торба А.А.* Математические модели датчиков шума // Прикладная радиоэлектроника. 2007. Т.6., №2, с.277-281. 2. *Патент* Украины № 68912 А, Бюл. № 8 от 16.08.2004. 3. *Патент* Украины № 61439 А, Бюл. № 11 от 17.11.2003. 4. *Торба А.А.*, *Елаков С.Г.*, *Степченко А.З.* Генерация равновероятных случайных последовательностей на основе физических датчиков // Радиотехника: Всеукр. межвед. науч.-техн. сб. 2001. Вып. 119, с.108-113. 5. *Патент* Украины № 36108 А, Бюл. № 3 от 16.04.2001

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 11. 02. 2008