УДК 621.391

А.В. ИВАШКО, к.т.н., ***М.Н. СОЛОЩУК***, к.т.н.,
О.В. АЛТУХОВА, студентка, ***А.В. СТЕПАНЕНКО*** (г. Харьков)

К ОЦЕНКЕ БЫСТРОДЕЙСТВИЯ ПЛИС-РЕАЛИЗАЦИЙ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ТАБЛИЦ

У статті розглянуті методи генерації псевдовипадкових послідовностей та таблиць. Запропоновано генерувати псевдовипадкові таблиці на основі двовимірного матричного зсувного регістру зі зворотними зв'язками. Обґрунтовано вибір елементної бази для реалізації генераторів. Оцінено часові характеристики генераторів на основі програмованих логічних інтегральних схем.

In proposed article pseudorandom sequences and tables generation methods are considered. Pseudorandom tables generation on the base of two-dimensional linear feedback shift registers are proposed. Elementary basis selection is grounded. Time characteristics of FPGA-based generators are estimated.

Псевдослучайные последовательности (ПСП), порождаемые сдвиговыми регистрами с обратными связями, находят широкое применение для измерения дальности в радиолокации, кодирования речи, обнаружения ошибок, модуляции, синхронизации, тестирования систем управления [1]. Наиболее широко распространены линейные рекуррентные последовательности, порождаемые сдвиговыми регистрами с линейными обратными связями, например, М-последовательности, последовательности Голда, Касами. Как правило, такие последовательности имеют близкую к дельтаобразной автокорреляционную функцию.

В то же время, для имитации шумов в видеосистемах, моделирования двумерных объектов, тестирования многоканальной связной и радиолокационной аппаратуры иногда возникает необходимость генерации псевдослучайных таблиц (ПСТ), то есть двумерных таблиц со спектрально-корреляционными свойствами, близкими к таковым у ПСП. Анализ известных методов генерации ПСП и ПСТ показал, что наиболее эффективной структурой для этого являются матричные сдвиговые регистры (*МСР*) [2]. Матричные генераторы предназначены для синтеза следующих типов ПСП и ПСТ:

М-, С-последовательностей, последовательностей Голда и их сумм;

последовательностей псевдослучайных таблиц и таблиц, близких по свойствам к псевдослучайным.

Структурные особенности матричных генераторов ПСП позволяют с их помощью генерировать системы перечисленных классов последовательностей, что делает их использование наиболее целесообразным в многоканальных цифровых системах.

Наиболее эффективным методом генерирования ПСТ представляется предложенный в [2] алгоритм. Матричный генератор ПСП, являясь реализацией автономной матричной линейной последовательностной машины (ЛПМ), формирует последовательности матриц над полем GF(P) следующим образом

$$S[i+1] = A*S[i]*B \ (\ i= 0,1,2,...,T_S-1), \qquad (1)$$

где $S[0] = S_0$, $S[i]$, $S[i+1]$ – матрицы начального, предыдущего и последующего состояний матричной ЛПМ размера $n \times m$, A и B – характеристические квадратные матрицы ЛПМ порядка n и m соответственно, T_S – период последовательности состояний. Элементы всех матриц принадлежат конечному полю $GF(p)$, где p – простое число, как правило, $p = 2$. Перечисленные выше ПСП образуются, например, как последовательности состояний элементов, столбцов (строк) или блоков матриц $S[i]$.

В качестве примера рассмотрим случай

$$A=\begin{bmatrix}0&0&1&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{bmatrix}, B=\begin{bmatrix}0&1&0&0&0\\0&0&1&0&0\\1&0&0&1&0\\0&0&0&0&1\\1&0&0&0&0\end{bmatrix}, S[0]=\begin{bmatrix}0&0&0&0&1\\0&0&0&0&1\\0&0&0&0&1\\0&0&0&0&1\end{bmatrix}$$

тогда

$$S[1] = A*S[0]*B(\mathrm{mod}\,2) = \begin{bmatrix}0&0&0&0&0\\1&0&0&0&0\\1&0&0&0&0\\1&0&0&0&0\end{bmatrix},$$

$$S[2] = A*S[1]*B(\mathrm{mod}\,2) = \begin{bmatrix}0&0&0&0&0\\0&0&0&0&0\\0&1&0&0&0\\0&1&0&0&0\end{bmatrix}$$ и т.д.

Таким образом, произошла циклическая перестановка столбцов влево, а строк - вверх по схеме, изображенной на рис. 1.

Заметим, что информация внутри матрицы $S[i]$ сдвинулась вдоль диагоналей, идущих справа-снизу влево-вверх. Схемная реализация МЛПМ, выполняющей циклическую перестановку строк и столбцов, представляет собой матричный сдвиговый регистр. Реализация МСР зависит от соотношения чисел n и m. Нетрудно заметить, что если наибольший общий делитель $(n, m) = 1$, то МСР вырождается в кольцевой регистр длины nm.

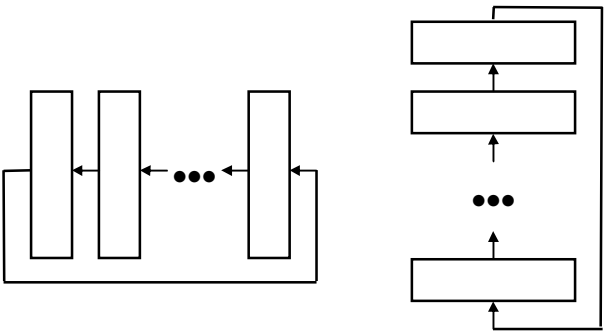

Рис. 1. Схема циклического сдвига столбцов и строк матрицы *S*

При построении матричных генераторов ПСП и ПСТ следует указать критерии, предъявленные к их аппаратным реализациям. Остановимся на следующих трех основных критериях:

- скорость генерации (большинство систем, использующих подобные устройства, предназначены для работы в реальном масштабе времени);
- минимальные аппаратные затраты (многофункциональность систем, имеющих в своем составе спецвычислители для генерации ПСП, требует от них минимальных размеров, невысокой стоимости, высокой технологичности);
- высокая гибкость при широком ассортименте классов ПСП (при работе спецвычислителей в условиях высокого уровня помех и широкого применения различных типов ПСП к данным устройствам предъявляются требования легкой перестраиваемости структур в ходе функционирования).

Элементной базой наилучшим образом удовлетворяющей указанным критериям, являются программируемые логические интегральные схемы (ПЛИС), удобная в освоении и применении элементная база, альтернативы которой зачастую не найти. С появлением современных ПЛИС появилась возможность создания высокопроизводительных и гибких генераторов достаточно высокого порядка. При этом ПЛИС благодаря особенностям своей архитектуры позволяют достигнуть наилучших показателей производительности по сравнению с другими способами реализации.

В работе были рассмотрены ПЛИС-реализации одномерных и двумерных генераторов ПСП. При анализе устройств использовались такие инструментальные средства как *Active-HDL*, *FPGA Express*. В одномерных сдвиговых регистрах были реализованы регистры разрядностей 8, 16, 24, 32, 48, 64. Для двумерного случая реализованы матрицы размерностей 4x4, 8x8, 12x12, 16x16, 20x20.

В среде *Active-HDL* линейный СРОС (сдвиговый регистр с обратной связью) представлен в следующем виде. Описаны порты *nWR*1, *nWR*2 – по первому порту осуществляется разрешение записи начального состояния регист-

ра (0-разрешено, 1-запрещено), по второму разрешение записи обратных связей регистра. Порты *A* и *q* (имеют тип *BIT_VECTOR*) – через них идет запись начального состояния и обратных связей. *Sch* – выход регистра.

Двумерный СРОС имеет три порта *nWR*1, *nWR*2, *nWR*3. На входы *nWR*1 подается размерность регистра. Второй и третий порты отвечают за разрешение записи столбцов либо строк матрицы. Через порт *DI* вводится управляющая информация, определяющая, какие сигналы будут подаваться на порты *nWR*1, *nWR*2, *nWR*3 – структура обратной связи, строка либо столбец. Порт *AD* отвечает за выбор номера строки или столбца, в совокупности с *RnC*. Порт *DO* является выходом с него можно считать значения выбранной строки или столбца. Порт *OE* разрешает выдачу информации с *DO*.

На рис. 2, 3 показана результат моделирования линейного СРОС при помощи системы *FPGA Express*, в левом столбце отображается частота, выбранная по умолчанию программы, а в правом показана частота, на которой устройство может в действительности работать. Графически результаты моделирования отображены на рис. 4.

	Name	Clock	Req. Freq (MHz)	Est. Freq (MHz)
1	<default>	20/0/10		
2	/"lfsr-Optimized"/clock		50	38

	Name	Clock	Req. Freq (MHz)	Est. Freq (MHz)
1	<default>	20/0/10		
2	/"lfsr-Optimized"/clock		50	30

	Name	Clock	Req. Freq (MHz)	Est. Freq (MHz)
1	<default>	20/0/10		
2	/"lfsr-Optimized"/clock		50	30

	Name	Clock	Req. Freq (MHz)	Est. Freq (MHz)
1	<default>	20/0/10		
2	/"lfsr-Optimized"/clock		50	30

	Name	Clock	Req. Freq (MHz)	Est. Freq (MHz)
1	<default>	20/0/10		
2	/"lfsr-Optimized"/clock		50	30

	Name	Clock	Req. Freq (MHz)	Est. Freq (MHz)
1	<default>	20/0/10		
2	/"lfsr-Optimized"/clock		50	25

Рис. 2. Тактовые частоты линейных сдвиговых регистров на основе ПЛИС размерностью 8, 16, 24, 32, 48, 64 бит

	Name	Clock	Req. Freq (MHz)	Est. Freq (MHz)
1	<default>	20/0/10		
2	/"Matrix4-Optimized"/C		50	12

	Name	Clock	Req. Freq (MHz)	Est. Freq (MHz)
1	<default>	20/0/10		
2	/"Matrix8-Optimized"/C		50	8

	Name	Clock	Req. Freq (MHz)	Est. Freq (MHz)
1	<default>	20/0/10		
2	/"Matrix12-Optimized"/C		50	7

	Name	Clock	Req. Freq (MHz)	Est. Freq (MHz)
1	<default>	20/0/10		
2	/"Matrix16-Optimized"/C		50	5

	Name	Clock	Req. Freq (MHz)	Est. Freq (MHz)
1	<default>	20/0/10		
2	/"Matrix20-Optimized"/C		50	5

Рис.3. Тактовые частоты двумерных линейных сдвиговых регистров размерностью 4x4, 8x8, 12x12, 16x16, 20x20 бит

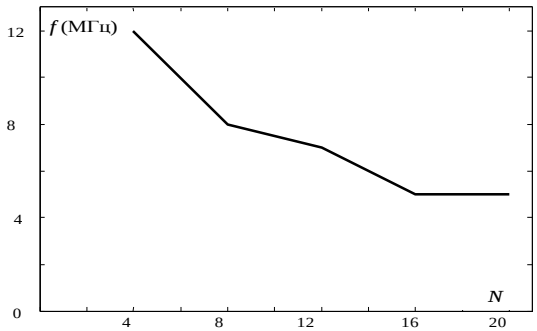

Рис.4. Зависимость максимально допустимой частоты генерации двумерного генератора ПСТ от размерности матрицы

В дальнейшем представляется целесообразным анализ ПЛИС-реализаций нелинейных генераторов ПСТ.

Список литературы: 1. *Мак-Вильямс Ф. Дж., Слоан Н.Дж.А.* Псевдослучайные последовательности и таблицы. - Тр. Ин-та инженеров по электротехнике и радиоэлектронике, 1976, 64, № 12, с. 80-95. **2.** *Солощук М.Н.* Анализ и синтез автономных матричных линейных последовательностных машин. Дис...к.т.н., Харьков, 1985.

Поступила в редколлегию 08.12.08