Математические структуры и моделирование
2010, вып. 21, с. 37–43

УДК 004.3

РЕАЛИЗАЦИЯ ГЕНЕРАТОРА СЛУЧАЙНЫХ ЧИСЕЛ НА БАЗЕ ЗВУКОВОЙ КАРТЫ

Д.Б. Беспалов, С.В. Белим

Работа посвящена созданию аппаратного генератора случайных последовательностей на основе интегрированной звуковой карты. Проводится тестирование генерируемых последовательностей.

Введение

Потребности в последовательностях случайных чисел возникают в самых разных областях знаний. Основные из них – моделирование, численный анализ, программирование, теория принятия решений и теория игр. Для всех этих целей вполне пригодным оказывается метод генерации псевдослучайных чисел, который способен выдавать последовательности с внушительной величиной периода и распределением, сколь угодно близким к заданному. Случайные числа находят свое применение и в криптографии. С их помощью происходит генерация ключей в большинстве криптопротоколов, случайных параметров сеансов связи в протоколах аутентификации, значений параметров многих систем ЭЦП и т. д. В этом случае накладывается дополнительное ограничение независимости в совокупности всех получаемых значений случайных чисел, что фактически означает невозможность (или вычислительную неэффективность) получения новых значений случайных чисел по известной части последовательности. Лишь немногочисленный класс генераторов ПСП удовлетворяет этому требованию; как правило, такие генераторы по-прежнему обладают строго детерминированным алгоритмом, однако функция генерации необратима, что затрудняет нахождение зависимостей внутри последовательности. В подобных ситуациях предпочтительнее использовать генератор истинно случайных чисел, реализуемый с помощью некоторого источника внешней энтропии. Под таким источником мы будем понимать некий физический процесс, параметры которого в каждый момент времени очень сложно предсказать. Известно множество реализаций таких аппаратных генераторов, в том числе достаточно остроумных, среди них плата с шумящим диодом, ПЗС-матрица в затемненной камере, датчик радиоактивного фона и многие другие. Одним из недостатков аппаратных генераторов является их относительно высокая стоимость, связанная с покупкой и обслуживанием необходимого оборудования; программные же генераторы

Омский государственный университет им. Ф.М. Достоевского.
E-mail: sbelim@mail.ru

лишены этих неудобств. Одной из базовых задач данного исследования являлся поиск аппаратных средств, входящих в состав большинства типовых конфигураций персональных и рабочих компьютеров по умолчанию и являющихся источником некоторой внешней энтропии. В данном случае стоимость генератора случайных чисел состояла бы исключительно из стоимости ПО для калибровки устройства и считывания значений. В качестве такого оборудования была выбрана звуковая карта, в интегрированном варианте присутствующая на абсолютном большинстве материнских плат. Источником энтропии в данном случае является шум на ее линейном входе. Основной задачей исследования являлось считывание этого шума и изучение его статистических характеристик, позволяющих сделать заключение о пригодности данного генератора для конкретных целей.

1. Реализация генератора случайных последовательностей

В качестве источника внешней энтропии рассматривается линейный вход звуковой карты [1]. Этот разъем предназначен для подключения источников аналогового звукового сигнала (таких как синтезатор или обычный кассетный магнитофон); такой сигнал, принятый на входе звуковой карты, переводится в последовательность байтов с помощью аналого-цифрового преобразователя. К действию полезного сигнала постоянно добавляется шум, вызванный электромагнитными наводками от других элементов цепи, тепловым шумом в цепях питания и прочими флуктуациями в подсистеме аналогового входа. С позиции поиска источника энтропии интерес представляет именно шум, а потому рассматривается линейный вход звуковой карты, на который не поступает никакого полезного сигнала. Считывание данных можно проводить с помощью любого интерфейса взаимодействия с устройством, например силами компонента DirectSound из коллекции DirectX. Так как мощность шума существенно ниже мощности полезного сигнала, предполагается, что в считываемых данных будут задействованы в основном младшие биты, причем максимальная битовая глубина шума напрямую зависит от качества устройства.

Для считывания данных с линейного входа звуковой карты была написана программа SoundRandom. Программа позволяет составить список устройств звукового захвата, действующих на компьютере, и выбрать в качестве источника любое из них. В качестве основных параметров считываемой последовательности можно задавать ее длину, а также количество младших битов, используемых для генерации. Программа позволяет провести базовую оценку равномерности распределения значений с помощью описательной статистики: среднее, сумма, дисперсия, эксцесс и пр. Код программы разделен на два отдельных модуля, отличающихся по функциональному назначению. Модуль взаимодействия с устройством реализует алгоритм считывания данных с линейного входа, используя функции DirectSound, среда разработки - Microsoft Visual C++ 6.0 [2]. Модуль графического интерфейса обеспечивает взаимодействие с пользователем, установку параметров, вывод графиков и отображение результатов, среда

разработки - Borland C++ Builder 6.

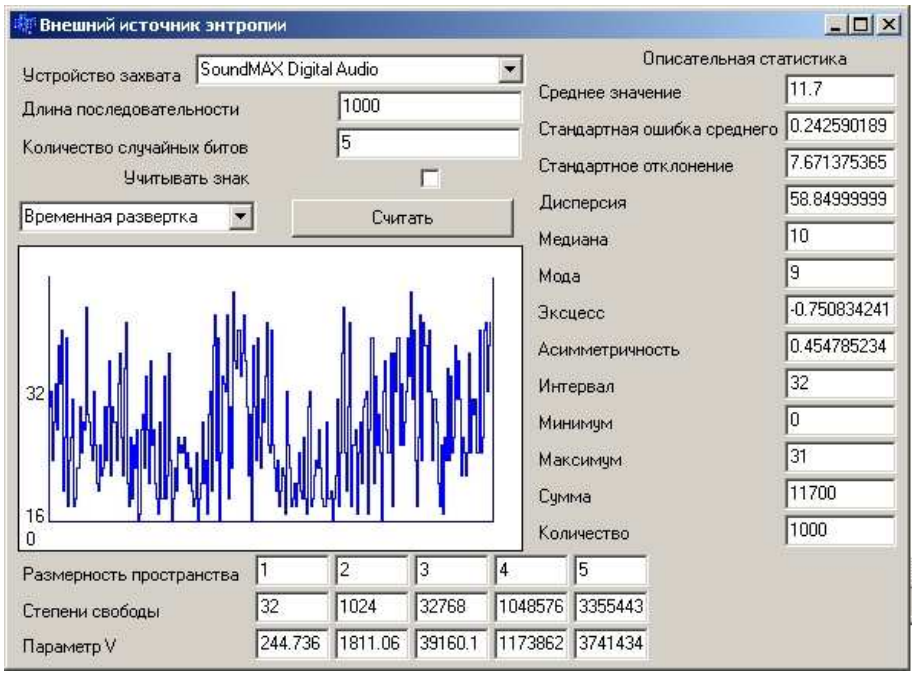

Рис. 1. Интерфейс программы SoundRandom

Алгоритм модуля взаимодействия с устройством состоит из функций, инициализирующих интерфейсы обращения к устройствам захвата и буферам записи, а также из функций, обрабатывающих начало и конец записи и очередное переполнение буфера. Интерфейс считывает по 44100 звуковых сэмплов в секунду, результат передается в вызывающий модуль, где для формирования последовательности используется необходимое количество младших битов сэмпла.

Функции, реализующие функционал модуля:

```
// Определение доступных устройств звукового захвата
HRESULT WINAPI DirectSoundCaptureEnumerate(
    LPDSENUMCALLBACK lpDSEnumCallback,
    LPVOID lpContext
);

// Создание объекта для взаимодействия с устройством
HRESULT WINAPI DirectSoundCaptureCreate(
    LPGUID lpGUID,
    LPDIRECTSOUNDCAPTURE *lplpDSC,
    LPUNKNOWN pUnkOuter
);

// Создание буфера для считывания данных
```

```
HRESULT CreateCaptureBuffer(
    LPDSCBUFFERDESC lpDSCBufferDesc,
    LPLPDIRECTSOUNDCAPTUREBUFFER lplpDirectSoundCaptureBuffer,
    LPUNKNOWN pUnkOuter
);

// Разметка буфера для определения переполнения
HRESULT SetNotificationPositions(
    DWORD cPositionNotifies,
    LPCDSBPOSITIONNOTIFY lpcPositionNotifies
);
```

2. Тестирование случайных последовательностей

Опираясь на данные одной лишь описательной статистики, нельзя утверждать, что полученная последовательность является равномерно распределенной случайной последовательностью (РРСП). Поэтому встает вопрос о проверке результатов с помощью ряда статистических критериев. Статистический критерий - это некая процедура, применяемая к количественным данным выборки. Каждый тест предназначен для проверки гипотезы H: «Заданная последовательность имеет равномерно распределенную случайную структуру». Для этого рассчитывается определенная статистика (своя для каждого теста), которая сравнивается с соответствующей статистикой РРСП. Величина отклонения полученного параметра от эталонного служит мерой «подозрительности» результата; начиная с некоторого предела отклонения последовательности отвергаются как неслучайные (или же распределенные иначе). Прохождение одного теста не гарантирует совпадения всех параметров последовательности с параметрами РРСП, поэтому очень важно прохождение целого набора тестов. Количество уже разработанных критериев велико, в сущности, их можно изобрести сколь угодно много. Хорошо зарекомендовавшими себя являются алгоритмы, описанные в «Искусстве программирования» Д. Кнута [1], а также тесты из большого набора «DieHard Test Battery» Д. Марсалья [4]. Опробовав полученные последовательности на достаточном количестве критериев, можно сделать вывод о ее пригодности к применению в криптостойких алгоритмах.

Для анализа статистических свойств сгенерированных числовых последовательностей создана программа Analizer. Она содержит набор из шести статистических критериев и механизм для обработки с их помощью последовательностей при любом заданном уровне группировки элементов [5,6]. По расчетным критериям программа представляет результат о прохождении данного теста и о категории, в которую попала тестируемая последовательность.

Критерии, реализованные в приложении: критерий хи-квадрат, критерий Колмогорова-Смирнова, критерий интервалов, покер-критерий, критерии распределения на плоскости и в пространстве.

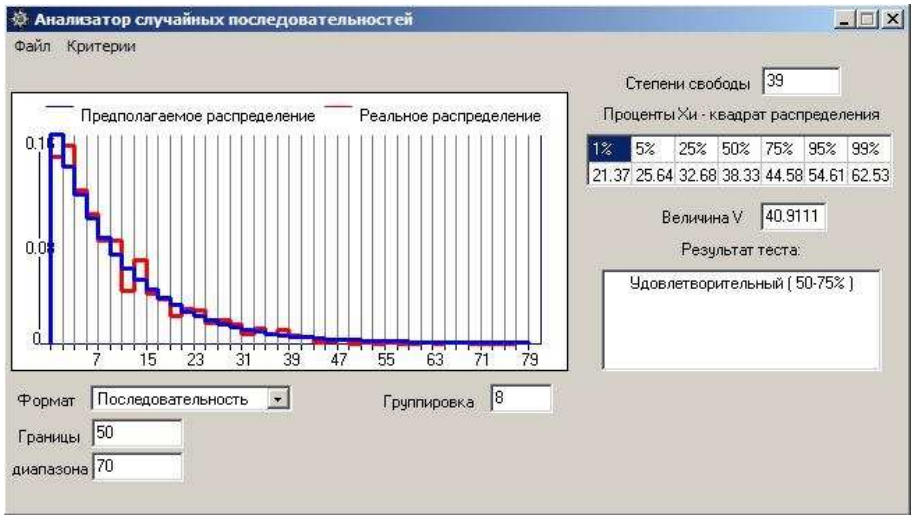

Рис. 2. Интерфейс программы SoundRandom

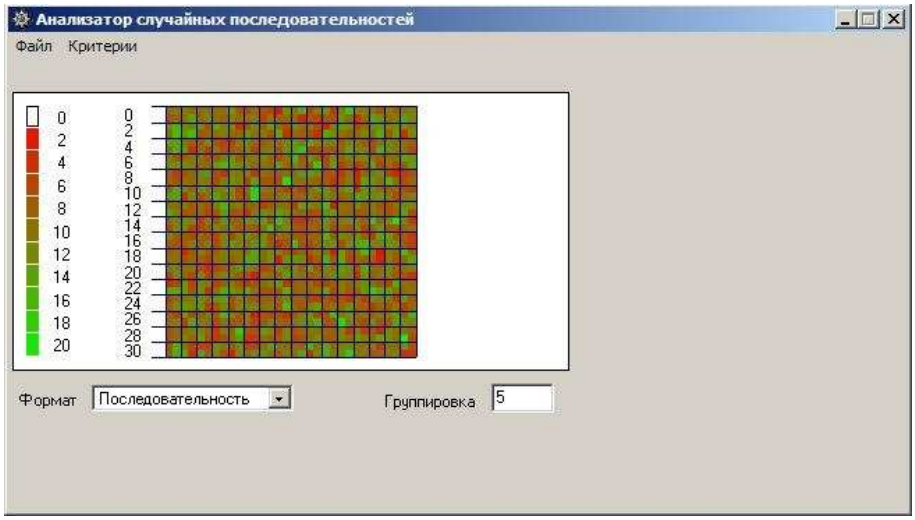

Рис. 3. Интерфейс программы SoundRandom

Испытания проводились на нескольких типах звуковых карт, все экземпляры были в интегрированном исполнении. Отсутствие сигнала на линейном входе карты контролировалось. С каждого устройства было считано по три последовательности длиной 100000 бит. Результаты применения тестов приведены в таблице; критерии, выдавшие неоднозначный ответ, отмечены цветом. Как видно, большинство тестов проходятся благополучно.

Картам в таблице присвоены следующие номера: 1) Realtek ALC662, 2) CMI8738/C3DX PCI, 3) SoundMax Digital Audio, 4) VIA AC97 Audio Chipset, 5) ADI AD1986A HD Audio. Набор тестов: T1 - хи-квадрат, T2 - критерий Колмогорова-Смирнова, T3 - критерий интервалов, T4 - покер-критерий. Параметры группировки: (1) - по 1 биту, (2) - по 2 бита, (3) - по 3 бита, (4) - по 4 бита.

Таблица 1. Результаты проверки критериев

посл	T1(1)	T2(1)		T3(1)	T4(1)	T1(2)	T2(2)		T3(2)	T4(2)
1 - 1	4.17	0	1.02	13.34	0.48	6.79	0	0.76	36.35	5.3
1 - 2	2.48	0.79	0	24.64	0.14	2.85	0.54	0	33.25	7.79
1 - 3	0	0.03	0	19.8	0.65	0.12	0.08	0.02	39.19	6.18
2 - 1	0	0	0.01	64.46	2.07	0.49	0.04	0.16	35.87	6.99
2 - 2	1.35	0	0.58	18.29	5.13	5.04	0	0.68	82.71	1.94
2 - 3	1.49	0	0.61	16.36	0.42	2.47	0	0.48	40.23	8.1
3 - 1	2.12	0	0.73	9.44	2.14	3.95	0	0.57	18.56	4.77
3 - 2	2.06	0.72	0	27.16	0.47	4.13	0.58	0	24.95	2.7
3 - 3	0.92	0.48	0	15.77	1.49	1.1	0.29	0	74.64	2.3
4 - 1	1.78	0	0.67	39.81	7.96	8.02	0.28	0.39	70.75	13.24
4 - 2	2.72	0	0.85	19.17	4.25	7.25	0	0.79	16.89	4.31
4 - 3	1.63	0	0.64	15.43	2.92	3.72	0	0.57	60.39	0.4
5 - 1	0.16	0	0.2	16.2	0.21	0.63	0.02	0.22	11.24	6.14
5 - 2	0.81	0	0.45	19.01	10.01	10.1	0.3	0.75	65.13	5.99
5 - 3	0.1	0.16	0	2.4	5.41	1.17	0.28	0.03	23.95	2.85

посл	T1(3)	T2(3)		T3(3)	T4(3)	T1(4)	T2(4)		T4(4)
1 - 1	8.48	0	0.58	112.87	9.66	16.08	0	0.5	17.62
1 - 2	5.09	0.4	0	62.23	5.68	24.95	0.47	0.19	4.38
1 - 3	4.04	0.1	0.35	34	6.85	19.57	0.26	0.14	4.31
2 - 1	11.92	0.18	0.52	67.17	1.63	20.37	0.32	0.25	1.87
2 - 2	6.14	0.04	0.48	31.78	2.99	19.09	0.28	0.44	8.11
2 - 3	4.82	0.05	0.33	26.13	7.05	14.21	0	0.47	5.07
3 - 1	14.94	0.24	0.82	158.96	8.3	23.15	0.24	0.39	3.12
3 - 2	8.2	0.3	0.14	32.7	3.6	12.4	0.33	0.1	2.06
3 - 3	14.94	0.48	0.23	35.22	3.53	16.07	0.32	0.08	6.58
4 - 1	13.76	0.14	0.54	251.39	10.57	30.49	0.25	0.53	3.35
4 - 2	13.55	0.07	0.64	75.7	7.28	22.51	0.22	0.34	2.56
4 - 3	5.2	0	0.37	50.83	1.79	19.02	0.13	0.45	1.71
5 - 1	4.97	0.26	0.18	64.59	6.57	16.22	0.16	0.27	3.87
5 - 2	13.36	0.37	0.38	66.44	5.25	43.13	0.45	0.37	2
5 - 3	3.74	0.24	0.11	40.26	1.43	15.98	0.43	0.15	5.31

В результате проведенных исследований был сделан вывод о том, что аналоговый вход звуковой карты обладает большим потенциалом в плане конструирования генераторов «истинно» случайных чисел. Основной положительный фактор в данном вопросе – цена построения работающего устройства; пользователь платит лишь за ПО, в аппаратной же части ему не нужно докупать никаких дополнительных приспособлений. В то же время генерируемые последовательности выдерживают все тесты на случайность и равномерность распределения, а потому годятся для применения в областях с повышенными требованиями к случайным числам. Также данный способ отличается большой стойкостью к возможным компрометациям со стороны конкурентов и недоброжелателей в случае, если будет предпринята попытка доказать прогнозируемость получаемой последовательности. Скомпрометировать генератор возможно только на специальным образом сконфигурированной системе, либо явно вмешавшись в его работу. С другой стороны, соблюдая определенные требования (спецификацию), можно быть уверенными в достаточной непредсказуемости генерируемых случайных чисел.

Литература

1. Юрьев Л. Генерация истинно случайных чисел на основе шума звуковых карт. URL: http://leo.yuriev.ru/114 (дата обращения: 01.02.2010).
2. Горнаков С.Г. DirectX 9: Уроки программирования на C++. Спб.: БХВ-Петербург, 2005. 400 с.
3. Кнут Д. Э. Искусство программирования. Том 2. Случайные числа. М.: Вильямс, 2002. 720 с.
4. Ylonen T. Introduction to Cryptography.
URL: http://algolist.manual.ru/defence/intro.php (дата обращения: 10.02.2010).
5. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей. М: КУДИЦ-ОБРАЗ, 2003. 240 с.
6. Marsaglia G. DIEHARD Statistical Tests. URL: http://stat.fsu.edu/ geo/diehard.html (дата обращения: 01.02.2010).