

УДК 004.056.55

Защита аудио сигнала с использованием скремблирования

Гончаров Н.О., студент

*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
кафедра «Информационная безопасность»*

Заикин М.А., студент

*Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
кафедра «Информационная безопасность»*

*Научный руководитель: Пристанский В.Л., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
v.a.matveev@bmstu.ru*

Введение

Целью работы является изучение и исследование эффективности метода защиты аудио сигнала при передаче по открытому аналоговому каналу связи с использованием скремблирования, а также программно-аппаратная реализация устройства аудиоскремблера с использованием программируемой логической интегральной схемы (ПЛИС) и язык описания аппаратуры интегральных схем *VHDL*.

В процессе выполнения работы был проведен цикл теоретических и экспериментальных исследований рациональных принципов построения, технических решений и параметров аппаратных и программных компонентов скремблера.

Скремблер – это устройство шифрования речи, используемое в системах телефонной связи. Шифрование выполняется разбиением спектра звукового сигнала на части (поддиапазоны) и дальнейшей частотной инверсией каждой из этих частей. Альтернативным аналоговому скремблированию речи является шифрование речевых сигналов, преобразованных в цифровую форму, перед их передачей. Этот метод обеспечивает более высокий уровень закрытия по сравнению с аналоговыми методами. В основе устройств, работающих по такому принципу, лежит представленные речевого сигнала в виде цифровой последовательности, закрываемой по одному из криптографических алгоритмов. Передача данных, представляющих дискретизированные отсчеты речевого сигнала или его параметров, по телефонным сетям, как и в случае устройств шифрования алфавитно-цифровой и графической информации, осуществляется через устройства, называемые модемами.

Основной целью при разработке устройств цифрового закрытия речи является сохранение тех ее характеристик, которые наиболее важны для восприятия слушателем. Одним из путей является сохранение формы речевого сигнала. Это направление применяется в широкополосных цифровых системах закрытия речи.

В последнее время сфера применения скремблирующих алгоритмов значительно сократилась. Это объясняется в первую очередь снижением объемов побитной последовательной передачи информации, для защиты которой были разработаны данные алгоритмы. Практически повсеместно в современных системах применяются сети с коммутацией пакетов, для поддержания конфиденциальности которой используются блочные шифры. А их криптостойкость превосходит, и порой довольно значительно, криптостойкость скремблеров.

1. Скремблирование и дескремблирование

Суть скремблирования заключается в побитном изменении проходящего через систему потока данных. Практически единственной операцией, используемой в скремблерах является XOR – "побитное исключающее ИЛИ". Параллельно прохождению информационного потока в скремблере по определенному правилу генерируется поток бит – кодирующий поток. Как прямое, так и обратное шифрование осуществляется наложением по XOR кодирующей последовательности на исходную. Генерация кодирующей последовательности бит производится циклически из небольшого начального объема информации – ключа по следующему алгоритму. Из текущего набора бит выбираются значения определенных разрядов и складываются по XOR между собой. Все разряды сдвигаются на 1 бит, а только что полученное значение ("0" или "1") помещается в освободившийся самый младший разряд. Значение, находившееся в самом старшем разряде до сдвига, добавляется в кодирующую последовательность, становясь очередным ее битом, как показано на рисунке 1.

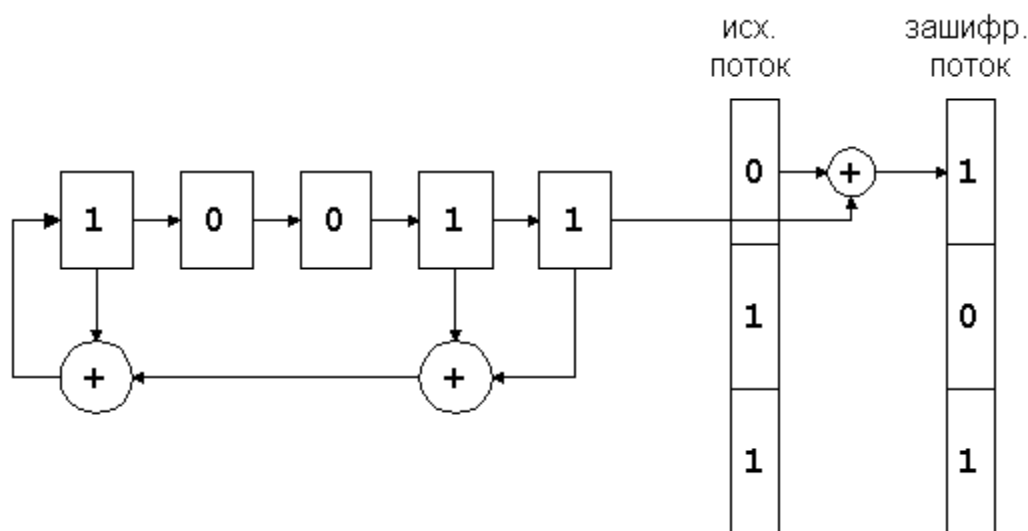


Рис. 1. Генерация кодирующей последовательности

Устройство скремблера предельно простое. Его реализация возможна как на электронной, так и на электрической базе, что и обеспечило его широкое применение в полевых условиях. Более того, тот факт, что каждый бит выходной последовательности зависит только от одного входного бита, еще более упрочило положение скремблеров в защите потоковой передачи данных. Это связано с неизбежно возникающими в канале передаче помехами, которые могут исказить только те биты, на которые они приходятся, а не связанную с ними группу бит, как это имеет место в шифрах с обратной связью. Для борьбы с помехами также широко используется избыточное кодирование, исправляющее ошибки.

Декодирование заскремблированных последовательностей происходит по той же самой схеме, что и кодирование. Именно для этого в алгоритмах применяется результирующее кодирование по "исключающему ИЛИ" — схема, однозначно восстанавливаемая при раскодировании без каких-либо дополнительных вычислительных затрат.

2. Проблема синхронизации и её решение

Главной проблемой шифров на основе скремблеров является синхронизация передающего (кодирующего) и принимающего (декодирующего) устройств.

При пропуске или ошибочном вставлении хотя бы одного бита вся передаваемая информация необратимо теряется. Поэтому, в системах шифрования на основе скремблеров очень большое внимание уделяется методам синхронизации.

На практике для этих целей обычно применяется комбинация двух методов:

а) добавление в поток информации синхронизирующих битов, заранее известных приемной стороне, что позволяет ей при не нахождении такого бита активно начать поиск синхронизации с отправителем;

б) использование высокоточных генераторов временных импульсов, что позволяет в моменты потери синхронизации производить декодирование принимаемых битов информации "по памяти" без синхронизации.

В нашем случае при работе со стерео аудиокодеком, проблема синхронизации может быть решена первым способом, с дополнительным контролирующим фактором, связанным с особенностью реализации схемы. Рассмотрим схему работы кодека представленную на рисунке 2.

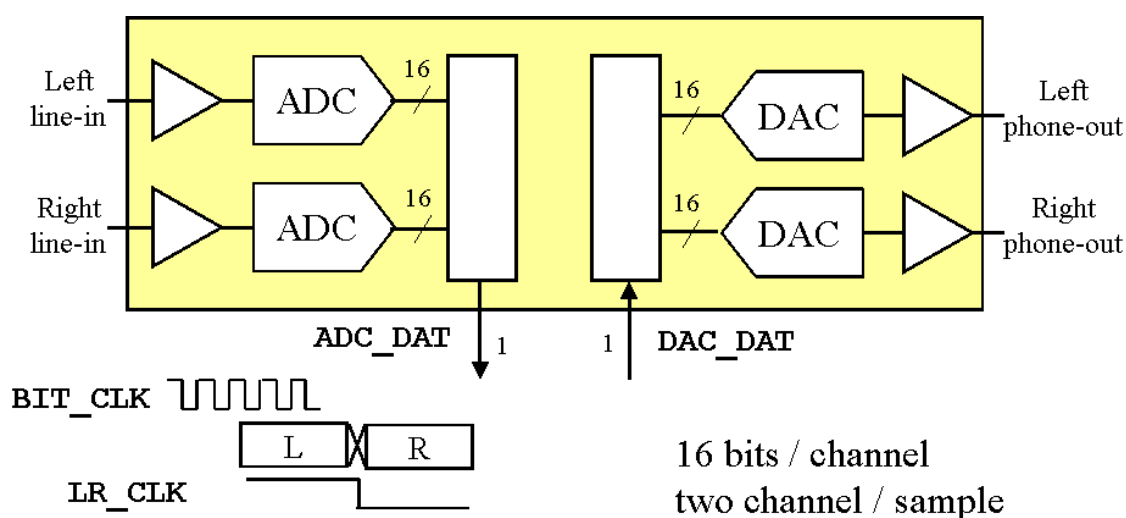


Рис. 2. Схема работы аудиокодека

Задав размер слова 16 бит и режим стерео, можно использовать изменение уровня сигнала LR_CLK (переключение левого/правого канала) для контроля синхронизации.

3. Аппаратная реализация

Функциональная схема аудиоскремблера состоит из аппаратной части, то есть реализуемую в виде совокупности расположенных на печатной плате интегральных микросхем которые соединены линиями связи, и программной части зашиваемую ПЛИС.

Взаимодействие блоков вне ПЛИС проиллюстрировано на рисунке 3.

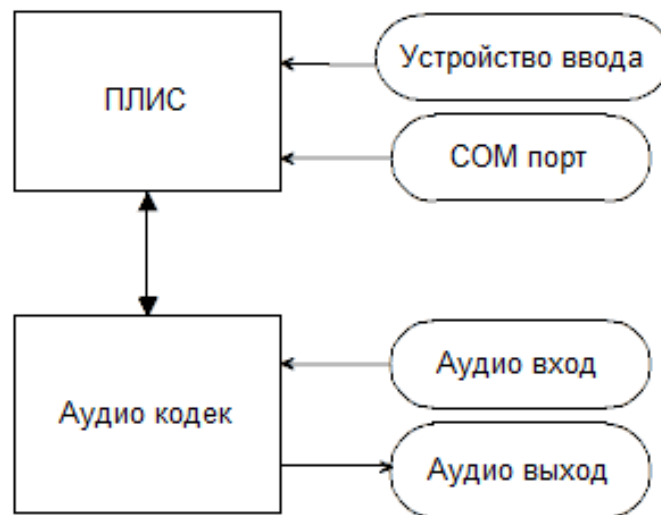


Рис. 3. Взаимодействие блоков вне ПЛИС

Центральным элементом схемы является ПЛИС, которая реализует управляющую логику. ПЛИС взаимодействует со всеми прочими элементами схемы. Причем все прочие элементы взаимодействуют между собой только через ПЛИС. Для взаимодействия с устройством ввода необходима 8-битная шина данных. Плис и аудио кодек взаимодействуют посредством интерфейса Digital Audio Interface (DAI). Конфигурирование кодека осуществляется по i2c шине.

4. Выбор ПЛИС

На данный момент ПЛИС представлены в виде микросхемы *FPGA*- и *CPLD*-структур. ПЛИС на *FPGA*-архитектуре основаны на ОЗУ и могут быть перепрограммированы бесконечное число раз. Но из-за этого у таких ПЛИС появляется существенный недостаток: при отключении питания программа теряется и для избежания ее потери нужен специальный конфигуратор. У ПЛИС с *CPLD*-структурой отсутствует проблема потери программы при отключении питания, т.к. они основаны на флэш-памяти. Поэтому программа может храниться постоянно, к тому же она может быть защищена битом секретности. Но вместе с тем у таких ПЛИС есть другой недостаток: микросхема может быть перепрограммируема ограниченное число раз.

Исходя из анализа достоинств и недостатков ПЛИС *FPGA*- и *CPLD*-структур и анализа тех задач, которые должна выполнять микросхема, были выбраны ПЛИС с *CPLD*-архитектурой.

Следующим критерием выбора была ёмкость ПЛИС. Общепринятой оценкой логической емкости ПЛИС является число эквивалентных вентилях, определяемое как

<http://sntbul.bmstu.ru/doc/622955.html>

среднее число вентилях "2И-НЕ", необходимых для реализации эквивалентного проекта на ПЛИС и базовом матричном кристалле (БМК). Эта оценка весьма условна, поскольку ПЛИС не содержит вентилях "2И-НЕ" в чистом виде, однако для проведения сравнительного анализа различных архитектур она вполне подходит.

Проведя анализ ПЛИС для выполнения работы была выбрана серия ИМС MAX фирмы Altera. Её основные характеристики приведены в таблице 1.

Таблица 1

Основные характеристики ПЛИС MAX II EPM570T100C5N

Семейство	MAX II
Количество логических ячеек	570
Количество I/O	76
Напряжение питания	1.15...3.465 В
Потребляемый ток	50 мА
Тип корпуса	FBGA100
Рабочая температура	0...85 °С

5. Выбор аудиокодека, генератора тактовых импульсов и разъемов

Аудиокодек на аппаратном уровне обозначает отдельную микросхему, которая кодирует и декодирует аналоговый звуковой сигнал в цифровой сигнал и наоборот при помощи аналогово-цифрового и цифро-аналогового преобразователей. Цифро-аналоговая конвертация происходит, когда компьютер посылает звук на внешние динамики, а аналого-цифровая конвертация происходит, когда звук подаётся на компьютер извне.

Воспользуемся аудиокодеком, Wolfson WM8731. Это полноценный мультибитный дельта-сигма I2S-кодек с произвольной опорной частотой дискретизации и продуманной системой аналогового усиления линейного и микрофонного сигнала до преобразователей АЦП, микрофонным предусилителем и буфером для наушников, что вполне удовлетворяет требования курсовой работы. Основные характеристики аудиокодека приведены в таблице 2.

Основные характеристики аудиокодека - Wolfson WM8731

Неравномерность АЧХ (от 40 Гц до 15 кГц), дБ:	+0.06, -0.05
Уровень шума, дБ (А):	-98.9
Динамический диапазон, дБ (А):	98.1
Нелин. искажения, %:	0.0017
Интермод. искажения, %:	0.0036
Взаимопроникновение каналов, дБ:	-96.4

Задержка сигнала при пассивной передаче с АЦП на ЦАП составляет 10 нс, в режиме скремблирования – 60 нс (частота, на которой работает аудио кодек - 18 МГц).

В качестве генератора тактовых импульсов будем использовать ИМС с кварцевым резонатором. Для работы ПЛИС необходим внешний генератор тактовых импульсов с частотой 50 МГц. Для подключения к ПК по протоколу RS232 был выбран разъем DB-9F. Для подключения аудио устройств были выбраны 2 аудио разъема TRS ¼.

Программный код прошивки для ПЛИС был реализован на языке описания аппаратуры интегральных схем *VHDL*.

В ходе разработки конечного изделия, была проведена работа с использованием отладочной платы *Altera Cyclone II Starter Kit*. Функциональная схема аудиоскремблера, разработанная с помощью программы для построения схем *Schemagee 3.05*, приведена на рисунке 4.

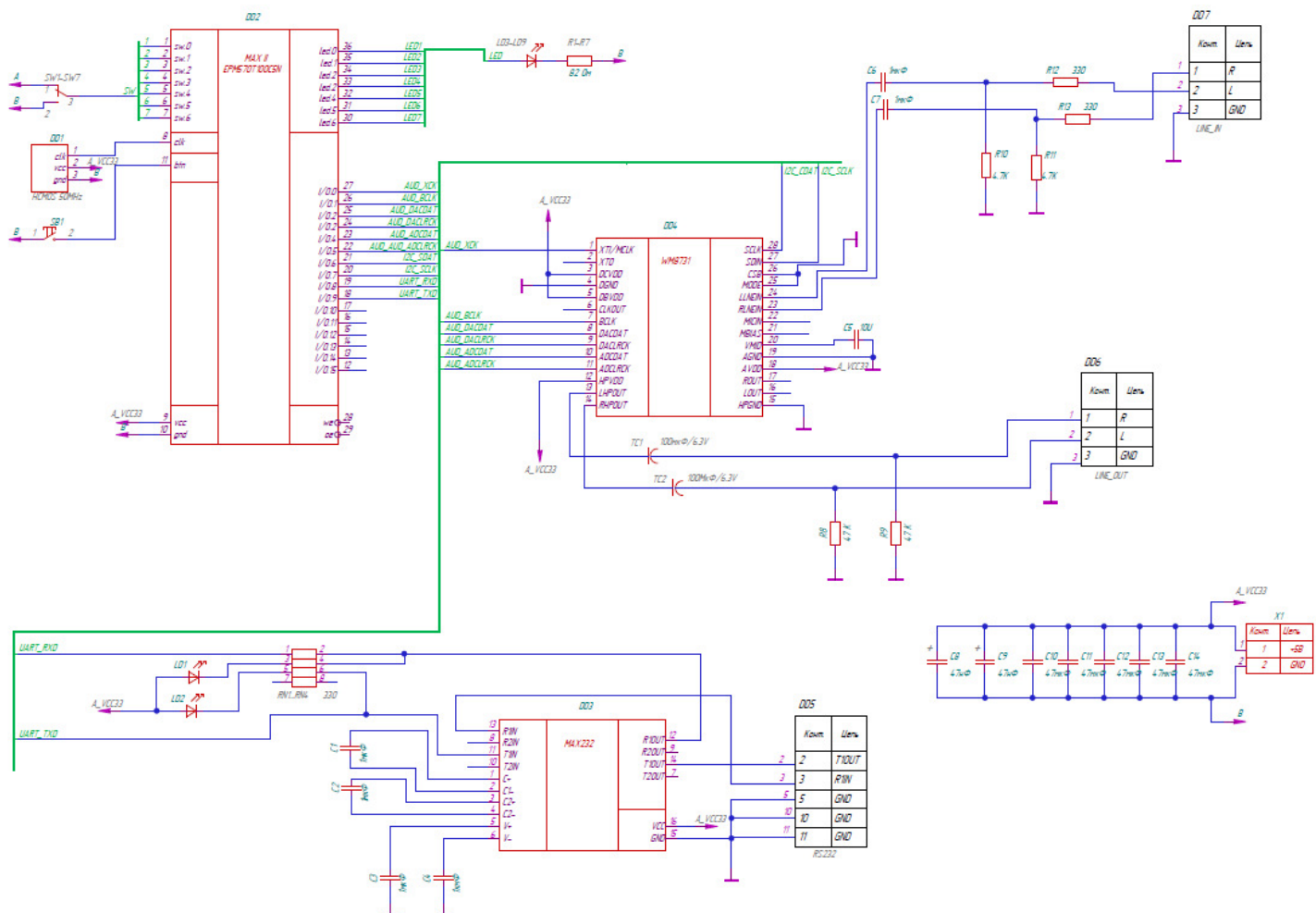


Рис. 4. Функциональная схема аудиоскремблера

Заключение

Общим недостатком такого типа скремблеров является наличие фона с частотой кодирования в составе восстановленного сигнала. Однако тщательное налаживание скремблера позволяет добиться практически полной маскировки фона полезным сигналом.

Налаживание схемы производят подключив выход кодера к входу декодера. В скремблере используются современные операционные усилители. К остальным деталям особых требований не предъявляется.

Список литературы

1. Г.И. Волович. Схемотехника аналоговых и аналого-цифровых устройств. М. : Додэка-XXI, 2011. 528 с.
2. Е. И. Куликов, А. П. Трифионов. Оценка параметров сигналов на фоне помех. М.: Сов. радио, 1978. 254 с.

3. Д.А. Поспелов Логические методы анализа и синтеза схем. М.: Энергия, 1974. 368 с.
Микропроцессоры и микропроцессорные комплекты интегральных схем: Справочник.
В 2-х т./В.- В.В. Абрайтис, Н.Н. Аверьянов, А.И. Белоус др.: под. ред. В.А Шахнова. -
М.: Радио и связь, 1988, т. 1- 368с.. т. 2- 368 с.