УДК 004.056.55

Разработка аудиоскремблера для защиты при передаче аудиосигнала

© Н.О. Гончаров, М.А. Заикин

МГТУ им. Н. Э. Баумана, Москва, 105005, Россия

Задачи обеспечения конфиденциальности передаваемой информации всегда стоят на первом месте, поэтому целью работы было изучение и исследование эффективности метода защиты аудиосигнала при передаче по открытому аналоговому каналу связи с использованием скремблирования, а также программно-аппаратная реализация устройства аудиоскремблер с использованием программируемой логической интегральной схемы (ПЛИС) и языка описания аппаратуры интегральных схем VHDL.

В процессе выполнения работы был проведен цикл теоретических и экспериментальных исследований, рациональных принципов построения технических особенностей и параметров аппаратных и программных компонентов скремблера, а также выбор оптимального решения для дальнейшей практической реализации. Результатом исследования стал рабочий прототип устройства, который был реализован на ПЛИС Altera Cyclone II Starter Kit, с использованием языка описания аппаратуры интегральных схем VHDL.

Ключевые слова: аудиоскремблер, защита информации, скремблер.

Введение. Целью работы является изучение и исследование эффективности метода защиты аудиосигнала при передаче по открытому аналоговому каналу связи с использованием скремблирования, а также программно-аппаратная реализация устройства «аудиоскремблер» с использованием программируемой логической интегральной схемы (ПЛИС) и языка 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 представление речевого сигнала в виде цифровой последовательности, закрываемой по одному из криптографических алгоритмов. Передача данных, представляющих дискретизированные отсчеты речевого сигна-

ла 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, что 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.

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 («02 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 рис. 1.

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 передачи 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.

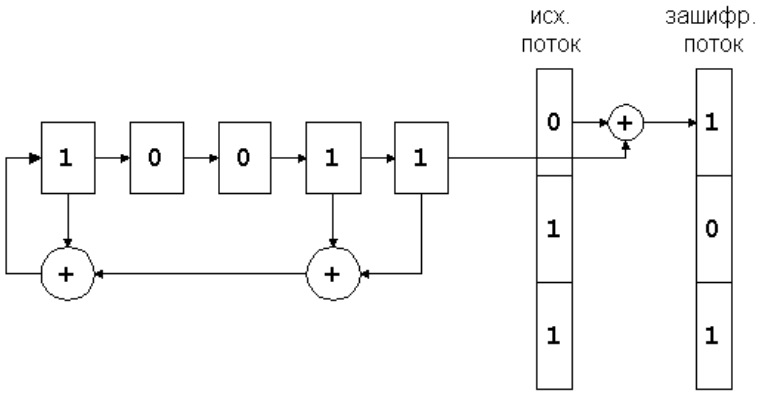

Рис. 1. Генерация кодирующей последовательности

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 восстановимая при раскодировании без каких-либо дополнительных вычислительных затрат.

Проблема синхронизации и ее 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 ненахождении 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 стереоаудиокодеком, проблема синхронизации может быть решена первым способом, с дополнительным контролирующим фактором, связанным с особенностью реализации схемы. Рассмотрим схему работы кодека, представленную на рис. 2. Задав размер слова 16 бит и режим стерео, можно использовать изменение уровня сигнала LR_CLK (переключение левого/правого канала) для контроля синхронизации.

Аппаратная реализация. Функциональная схема аудиоскремблера состоит из аппаратной части, реализуемой в виде совокупности расположенных на печатной плате интегральных микросхем (ИМС), которые соединены линиями связи, и программной части.

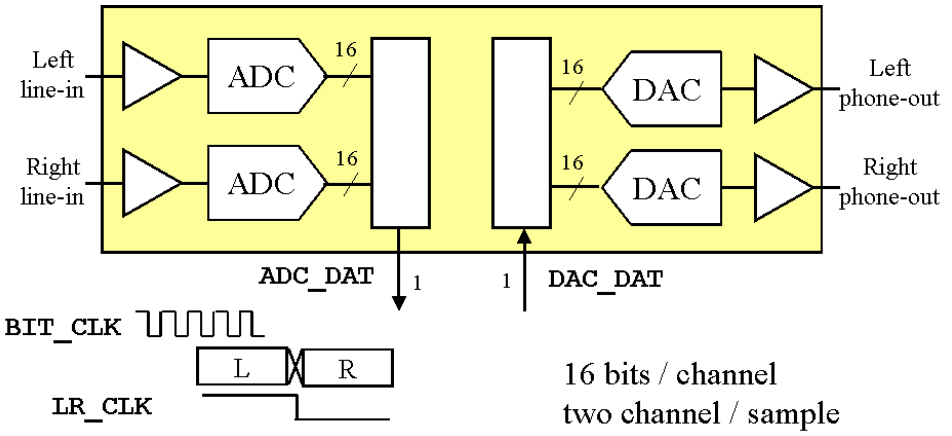

Рис. 2. Схема работы аудиокодека

Взаимодействие блоков вне ПЛИС проиллюстрировано на рис. 3.

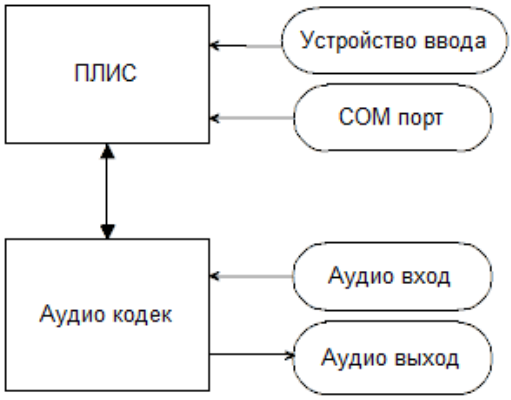

Рис. 3. Взаимодействие блоков вне ПЛИС

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 аудиокодек взаимодействуют посредством интерфейса Digital Audio Interface (DAI). Конфигурирование кодека осуществляется по i2c шине.

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 от-

сутствует проблема потери программы при отключении питания, так как 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 емкость ПЛИС. Общепринятой оценкой логической емкости ПЛИС является число эквивалентных вентилей, определяемое как среднее число вентилей «2И-НЕ», необходимых для реализации эквивалентного проекта на ПЛИС и базовом матричном кристалле (БМК). Эта оценка весьма условна, поскольку ПЛИС не содержит вентилей «2И-НЕ» в чистом виде, однако для проведения сравнительного анализа различных архитектур она вполне подходит.

После анализа ПЛИС для выполнения работы была выбрана серия ИМС MAX фирмы Altera. Ее основные характеристики приведены в табл. 1.

Таблица 1

Основные характеристики ПЛИС MAX II EPM570T100C5N

Семейство	MAX II
Количество логических ячеек	570
Количество I/O	76
Напряжение питания, В	1,15…3,465
Потребляемый ток, мА	50
Тип корпуса	FBGA100
Рабочая температура, °С	0...85

Выбор аудиокодека, генератора тактовых импульсов и разъемов. Аудиокодек на аппаратном уровне обозначает отдельную микросхему, которая кодирует и декодирует аналоговый звуковой сигнал в цифровой и наоборот с помощью аналого-цифрового и цифроаналогового преобразователей. Цифроаналоговая конвертация происходит, когда компьютер посылает звук на внешние динамики, а аналого-цифровая, когда звук подается 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 требованиям к курсовой работе. Основные характеристики аудиокодека приведены в табл. 2.

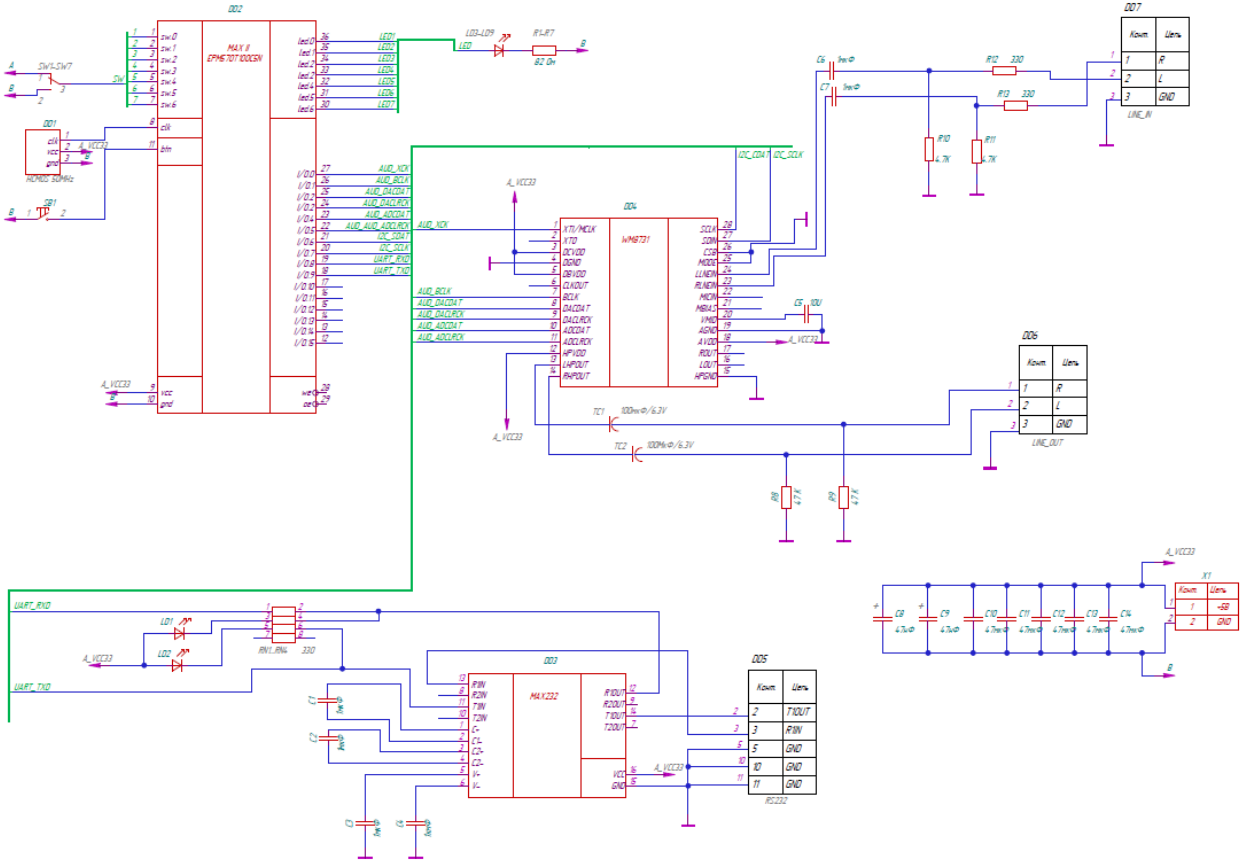

Рис. 4. Функциональная схема аудиоскремблера

Таблица 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
Нелинейные искажения, %	0,0017
Интермодуляционные 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 аудиокодек — 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 аудиоустройств были выбраны 2 аудиоразъема TRS 1/4.

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 рис. 4.

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

Результатом исследования стал рабочий прототип устройства, который был реализован на ПЛИС Altera Cyclone II Starter Kit, с использованием языка описания аппаратуры интегральных схем *VHDL*.

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 подключением выхода кодера к входу декодера. В скремблере используются современные операционные усилители.

Статья поступила в редакцию 28.06.2013

Ссылку на эту статью просим оформлять следующим образом:

Гончаров Н.О., Заикин М.А. Разработка аудиоскремблера для защиты при передаче аудиосигнала. *Инженерный журнал: наука и инновации*, 2013, вып. 11. URL: http://engjournal.ru/catalog/it/security/992.html

Гончаров Николай Олегович родился в 1990 г. Студент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. e-mail: goncharovkolya@list.ru

Заикин Михаил Андреевич родился в 1991г. Студент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана. e-mail: 3aikin@gmail.com