и другие. На генератор единовременно подаются два импульсных напряжения: одно – с импульсного модулятора, который формирует требуемую длительность зондирующего сигнала; другое – с генератора пилообразного напряжения (ГПН), который осуществляет частотную модуляцию на протяжении всего импульса. Необходимую стабильность частоты в схеме поддерживает система автоподстройки частоты (АПЧ) средней частоты линейно-частотной модуляции (ЛЧМ) сигнала и система автоматической подстройки закона модуляции. Принцип работы системы основан на сравнении выходного сигнала с эталонным. Если выходной сигнал не совпадает с эталонным, то вырабатывается сигнал ошибки, который отправляется на ГПН (генератор пилообразного напряжения). В следствии чего изменяется амплитуда пилообразного напряжения, следовательно и закон изменения частоты задающего генератора – в сторону уменьшения ошибки.

Запускающий импульс (зондирующий импульс поступивший с детектора) поступает на линию задержки. В то же время, на длительность зондирующего импульса, детектор отпирает ключ. Энергия зондирующего импульса через открытый ключ поступает на выпрямитель и запитывает конденсатор схемы. Напряжение конденсатора подается на генератор высокой частоты, считывающее устройство и генератор командного сигнала, однако энергия не расходуется, так как не поступало команды на запуск. Далее, линия задержки выдает запускающий импульс на генератор командного сигнала, эта информация попадает на считывающее устройство и генератор высокой частоты. Считывающее устройство отправляет сигнал на считывание блоку памяти и получает информацию в ответ, пересылая ее смесителю. Генераторы высокой частоты генерирует сигнал несущей частоты, направляет смесителю, откуда информация и энергия поступают на АЦП (состоящий и АИМ, генераторы тактовой частоты, квантователя и ИКМ), помехоустойчивый кодер. После всего этого, кодовые комбинации попадают отправляются на модулятор, преобразующий код в сигнал, подходящий для передачи через антенну.

С антенны сигнал поступает на линию задержки и далее происходит демодуляция, преобразуя сигнал в последовательность кодовых комбинаций. Декодер восстанавливает исходный код, обнаруживает и устраняет ошибки. Информация поступает на логическую схему. В это время источник питания запитывает логическую схему и позволяет записать информацию в блок памяти. Далее информация поступает на интерфейс связи. Т.к. у нас сетевой ридер, то информация поступает в систему электронной логистики с помощью Wi-fi технологии.

Переход от штрих-кодирования к радиочастотной идентификации является залогом успешного будущего складской автоматизации и логистики.

Список использованных источников:

1. Сандип Лахири. RFID. Руководство по внедрению. Пер. с англ. – М.: КУДИС-ПРЕСС. – 2007. – 312 с., илл.

2. Евменов В. П. Интеллектуальные системы управления: Учебное пособие. М.: Книжный дом “ЛИБРКОМ”, 2009. – 304 с.

3. Башмаков А. И., Башмаков И. А. Интеллектуальные информационные технологии: Учеб. пособие. – М.: Изд-во МГТУ им. Н. Э. Баумана, 2005. – 304 с.: ил. – (Информатика в техническом университете)

ИТЕРАТИВНО-КОНВЕЙЕРНЫЙ ПРОЦЕССОР ХЭШ-ФУНКЦИИ SHA-256 НА БАЗЕ ПЛИС

Ероховец В.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Станкевич А.В. – к.т.н.,доцент

Функция хеширования SHA-256 достаточно популярна последние несколько лет. Являясь относительно простой, она идеально подходит для самых разных целей. Существует множество различных подходов к реализации алгоритма, как программных, так и аппаратных. В докладе рассматривается аппаратная итеративно-конвейерная реализация, так как она занимает относительно небольшой объем ресурсов и является достаточно производительной.

В настоящее время достаточно остро стоит проблема сохранения конфиденциальности информации, а также корректности ее передачи. Целостность передаваемой информации можно контролировать при помощи сообщения, полученного путем обработки исходного послания используя хеш-функции.

Алгоритм хеширования SHA-256 относится к семейству алгоритмов SHA-2 (Secure Hashing Algorithm), разработчиком которого является Агентство национальной безопасности США.

Реализация данного алгоритма аппаратным способом значительно повышает скорость обработки данных по сравнению с программным.

Исходя из алгоритма, можно выделить две составные части реализации:

1) экспандер («расширитель»);
2) компрессор («уплотнитель»).

С помощью экспандера сообщение удлиняется для последующей обработки. А в компрессоре уже проходит эта обработка, которая предполагает в общем случае сжатие исходного сообщения до длины 256 бит.

Для того, чтобы получить более высокую тактовую частоту, необходимо уменьшить длину критического пути как в экспандере, так и в компрессоре, что достигается путем модификации канонической модели [2]. На рисунке 1 представлены модифицированные структурные схемы экспандера и компрессора:

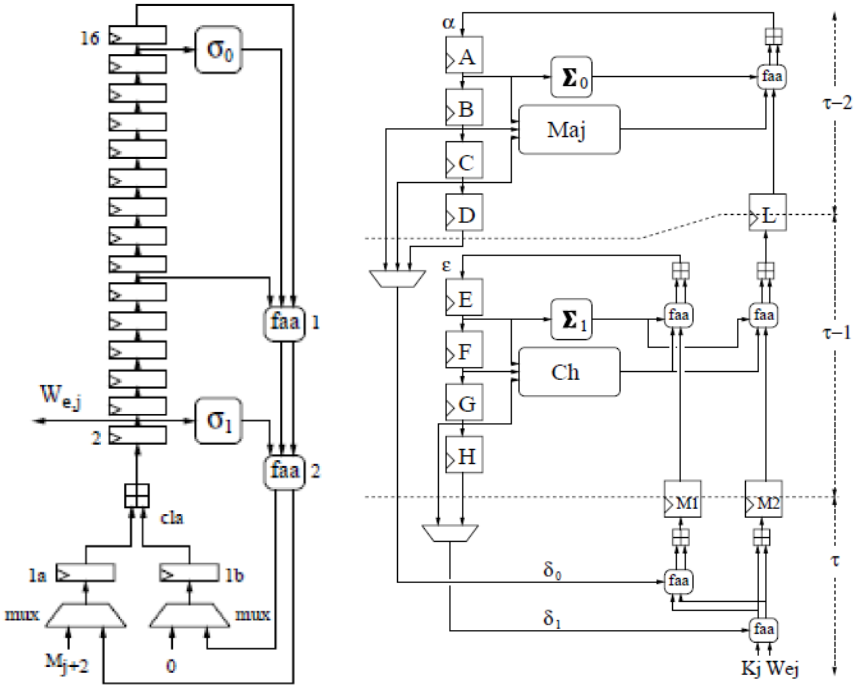

Рисунок 1 – Структурные схемы экспандера и компрессора соответственно [2]

Приведенное архитектурное решение реализуется на FPGA семейства Virtex 7 компании Xilinx. Проводятся исследования производительности и аппаратных затрат реализации.

Список использованных источников:

1. D. Eastlake 3rd., Motorola Labs/ T. Hansen – AT&T Labs, July 2006. – 108 P.
2. L. Dadda, M. Macchetti, J. Owen . An ASIC Design for a High Speed Implementation of the Hash Function SHA-256 (384, 512). Proc. of GLSVLSI '04 Proceedings of the 14th ACM Great Lakes symposium on VLSI, Boston, MA, USA — April 26 - 28, 2004. - ACM New York, NY, USA, 2004. – pages 421–425.
3. Wikipedia [Электронный ресурс]. – Электронные данные. – Режим доступа: https://ru.wikipedia.org/wiki/SHA-2

АППАРАТНАЯ ПЛАТФОРМА ДЛЯ ПРОТОТИПИРОВАНИЯ АЛГОРИТМОВ И АРХИТЕКТУР СЛУХОВЫХ АППАРАТОВ НА ОСНОВЕ СНК ZYNQ

Кивачук А.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Вашкевич М.И. – к.т.н.,доцент

В настоящее время около 1 миллиарда человек (16% населения мира) страдают потерей слуха. Большинство из них не имеют слухового аппарата либо недовольны качеством его работы. Необходимость в разработке новых и совершенствовании существующих алгоритмов обработки сигналов в слуховых аппаратах требует наличия соответствующих аппаратных платформ. Существует большое количество платформ для обработки сигнала, однако не хватает мобильных платформ, подходящих для реализации алгоритмов, необходимых для слуховых аппаратов. В работе представлена аппаратная