100% вероятностью.

2. Подтверждение обнаружительной способности для минимального дефекта, размером “*d*”, обнаруживаемого с вероятностью 95%. При этом *d* соответствует порогу обнаружения.

Последовательное определение вероятностей обнаружения дефектов с размерами, меньшими порога обнаружения. При этом последовательно рассматриваются дефекты, начиная с дефектов размером *d*-Δ*d*, с шагом Δ*d*, заканчивая дефектами, имеющими контраст 10%. Шаг Δ*d* может быть выбран, например, равным 50 нм. Согласно методике вероятность обнаружения дефектов связана с частотой обнаружения дефектов следующим образом:

$$P\left(\left|\frac{m}{n}-p\right|<\varepsilon\right)\geq 1-pq/n\varepsilon^2, \quad (1)$$

где *P* – вероятность нахождения обнаружения в интервале, *m* – число благоприятных исходов, *n* – общее число циклов сканирования, *p* – вероятность обнаружения дефектов, *q* – вероятность необнаружения дефектов, *ε* – размер доверительного интервала, *m*/*n* – частота события: «Обнаружение дефекта».

Отсюда получаем соотношения между вероятностью обнаружения *ε* и необходимым количеством *n* циклов сканирования фотошаблонов, которые приведены в таблице.

Вероятность обнаружения	0,005	0,01	0,05	0,1	0,1
Количество циклов *n*	38000	9500	380	95	24

Нужно отметить, что если воспользоваться теоремой Муавра-Лапласа, то можно получить существенно меньшие приближенные значения для числа циклов испытаний [2].

Точное определение вероятности обнаружения дефектов с размерами, меньшими порога обнаружения установки, позволяет оптимизировать процесс фильтрации ложных дефектов типа прокол и островок при автоматическом контроле топологии, а также повысить воспроизводимость контроля.

Предложенная методика позволяет точно определить количество испытаний, необходимых для подтверждения вероятности обнаружения дефектов при автоматическом контроле топологии и используется при разработке программ и методик испытаний всего спектра отечественного оборудования для автоматического контроля топологии СБИС и других изделий электронной техники.

Список использованных источников:

1. Аваков, С.М. Автоматический контроль топологии планарных структур / С.М. Аваков. – Минск : ФУАинформ, 2007. – 168 с.
2. Alfred, K.W. Resolution Engancement Techniques in Optical Lithography. SPIE PRESS, USA, 2001. – pp. 1–213.

СПЕЦИАЛИЗИРОВАННЫЙ ПРОЦЕССОР ШИФРОВАНИЯ СТАНДАРТА СТБ 34.11.31-2007

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

Мельников А. М.

Герасимович В. Ю. – ассистент

Рассмотрен один из возможных вариантов реализации специализированного процессора шифрования стандарта СТБ 34.11.31 на базе программируемых логических интегральных схем (ПЛИС) типа FPGA. Приводятся сравнительные характеристики различных реализаций стандарта.

Стандарт СТБ 34.11.31-2007[1] – определяет семейство криптографических алгоритмов шифрования и контроля целостности. Все алгоритмы данного стандарта деляться на 8 групп: шифрования в режимах простой замены, сцепления блоков, гаммирования с обратной связью и счетчика, алгоритмы выработки имитовставки, одновременного шифрования и имитозащиты данных, одновременного шифрования и имитозащиты ключа, а также хеширования. В данной работе будет рассмотрена аппаратная реализация шифрования в режиме гаммирования с обратной связью. Алгоритм рассчитан на шифрование блоков данных длиной 128 бит на 256 битый ключ. Шифрование осуществляется 8-ю раундами преобразований, применяемых к входным данным. При этом для одного блока применяются следующие базовые операции: сложение(80 32-разрядных операций), вычитание(16 32-разрядных операций), сложение по модулю 2(40 32-разрядных операций), циклический сдвиг вправо(56 32-разрядных операций с фиксированным сдвигом на 5,13 или 21 разряд), подстановка(224 8-разрядных операций).

Для реализации данного алгоритма была выбрана последовательная схема с параллелизмом вычислений на уровне такта шифрования, вычисления на t такте приведены на рисунке 2. Выбор последовательной схемы связан с присутствием в режиме гаммирования, обратной связи, не позволяющей реализовать полный конвейер. Параллелизм реализован при помощи конвейерной архитектуры блока

вычислений, который включает в себя повторяющиеся шаги одного такта алгоритма, функциональная схема блока приведена на рисунке 1.

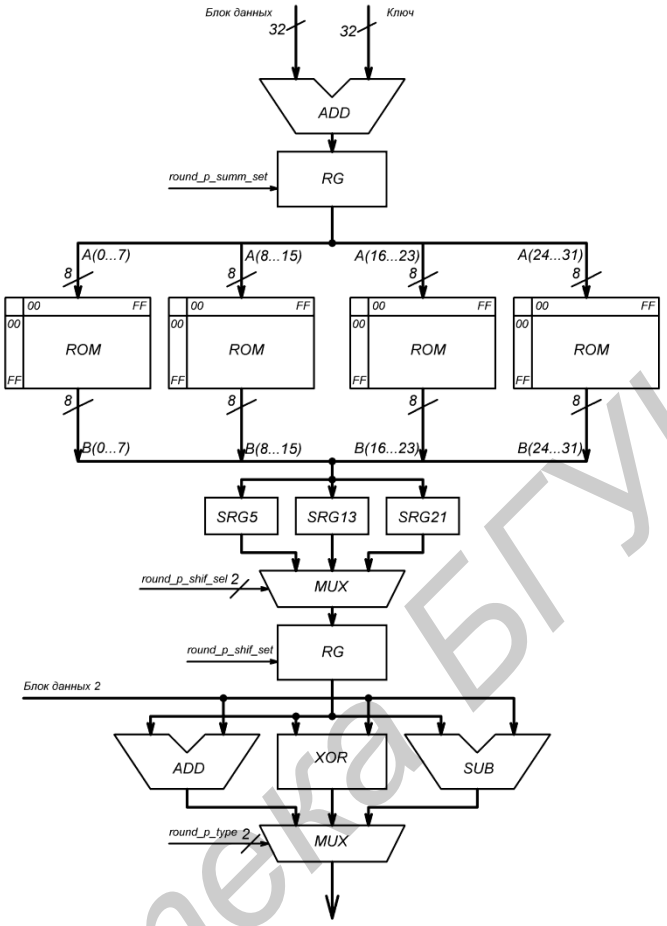

Рис. 1. Функциональная схема блока вычисления

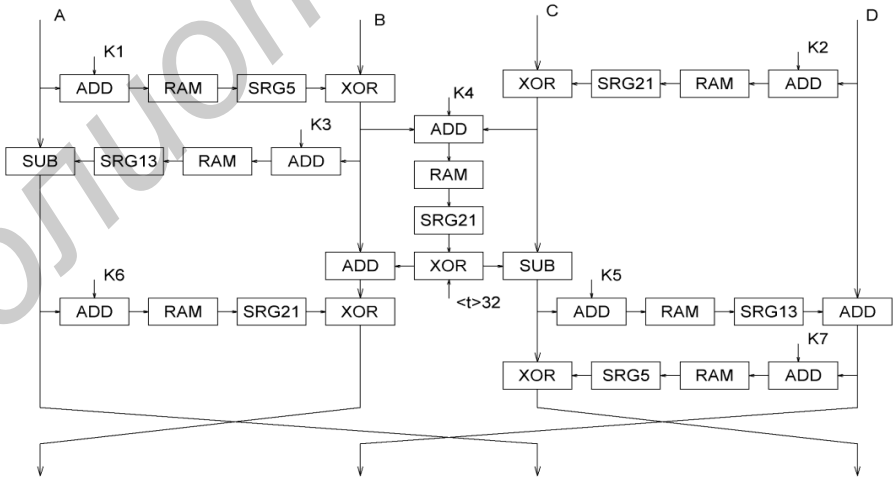

Рис. 2. Вычисления на t-м такте зашифрования

Для размещения проекта был выбран кристалл ПЛИС xc6vlx130t, семейства Virtex 6 компании Xilinx, для описания логики работы устройства использовался язык VHDL[2].

В таблицах 1 и 2 приведены результаты проектирования, а также их сравнения с результатами, указанными в материалах [3], [4] и [5]:

Таблица 1. Производительность некоторых реализаций алгоритма

Варианты реализации	Количество тактов	Тактовая частота устройства, МГц.	Производительность, Мбит/сек	Устройство

Belt_seq[3]	336	500	190,47	ПЛИС Spartan xc3s200
Belt_par[3]	211	500	289,59	ПЛИС Spartan xc3s200
Программная[5]	682	1000	187,68	Процессор Pentium III
Последовательная[4]	66	112,4	217,98	ПЛИС Virtex xc6vlx130t
Конвейерная[4]	114(1)	217,4	243,65(27 827)	ПЛИС Virtex xc6vlx130t
Уменьшенная конвейерная[4]	114(14)	217,4	243,65(1 987,6)	ПЛИС Virtex xc6vlx130t
С параллелизмом на уровне такта	225	454.54	258,58	ПЛИС Virtex xc6vlx130t

Примечание – Для конвейерных реализаций в скобках указанна производительность после заполнения конвейера, а также количество тактов необходимых для формирования каждого следующего результата.

Таблица 2. Аппаратные затраты при размещении на кристалле FPGA

Варианты реализации	Slices	Триггеров	LUTs	RAMs	Устройство
Belt_seq[3]	750	649	1392	9	ПЛИС Spartan xc3s200
Belt_par[3]	1070	302	2050	28	ПЛИС Spartan xc3s200
Последовательная[4]	423	847	1173	-	ПЛИС Virtex xc6vlx130t
Конвейерная[4]	9157	10209	14816	112	ПЛИС Virtex xc6vlx130t
Уменьшенная конвейерная[4]	4829	5598	7948	28	ПЛИС Virtex xc6vlx130t
С параллелизмом на уровне такта	399	1362	937	2	ПЛИС Virtex xc6vlx130t

Список использованных источников:

1. СТБ 34.101.31-2007. Государственный стандарт Республики Беларусь. Криптографические алгоритмы шифрования и контроля целостности.
2. Бибило, П. Н. VHDL. Эффективное использование при проектировании цифровых систем / П. Н. Бибило, Н .А. Авдеев. – М.: СОЛОН-Пресс, 2006. – с. 344
3. Поляков,А.С. Характеристики аппаратной реализации некоторых симметричных алгоритмов шифрования / А. С. Поляков, В. Е. Самсонов // Информатика : Ежеквартальный научный журнал, 2011. – №1.
4. Ланкевич, Ю. Ю. Процессор алгоритма шифрования «Belt» на базе ПЛИС / Ю. Ю. Ланкевич // Информационные технологии и системы 2013 (ИТС 2013) : материалы международной научной конференции, БГУИР, Минск, Беларусь, 23 октября 2013 г. / редкол.: Л. Ю. Шилин [и др.]. – Минск : БГУИР, 2013. – с. 190-191.
5. Агиевич, С. В. Алгоритм блочного шифрования BelT / С. В. Агиевич, В. А. Галинский, Ю. С. Харин, Н. Д Микулич. Управление защитой информации, т.6, №4, 2002. – с.407–412

СПОСОБ ФОРМИРОВНИЯ ВЫСОКОЧАСТОТНОЙ СОСТАВЛЯЮЩЕЙ СПЕКТРА СИГНАЛА В НИЗКОСКОРОСТНОМ АУДИОКОДЕРЕ

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

Герасимович В. Ю.

Петровский А. А.– д-р. техн. наук, профессор

Работа посвящена описанию варианта повышения качества реконструированного сигнала аудиокодера [1] при низких скоростях битового потока. Рассматривается способ формирования высокочастотной составляющей спектра выходного аудиосигнала путем копирования и масштабирования информации среднечастотной части спектра сигнала.

Принцип сжатия аудиоданных с потерями состоит в выделении из входной последовательностиданных, которые позволяют компактно представить и синтезировать на стороне декодера выходной сигнал. Основная задача кодера заключается в поиске наиболее важных для восприятия человеком параметров. Так как количество выбираемых данных ограничено скоростью битового потока (битрейта) аудиокодера, часть информации о входном сигнала теряется. В силу особенностей восприятия человеком аудиосигнала, высокочастотные компоненты спектра менееперцептуально важны, нежели низко- и среднечастотные [2]. Поэтому, при низких скоростях битового потока (т.е. малом количестве бит, выделяемых для передачи сигнала), параметры, соответствующие данной полосе могут быть проигнорированы и опущены, что повлечет за собой уменьшение качества реконструированного сигнала.Данный материал посвящен вопросу формирования высокочастотной составляющей спектра в аудиокодере на основе согласованной подгонки