ОСОБЕННОСТИ РЕАЛИЗАЦИИ ПРОЦЕССОРОВ АЛГОРИТМА КРИПТОГРАФИЧЕСКОГО ХЭШИРОВАНИЯ SHA-1 НА БАЗЕ FPGA-КЛАСТЕРОВ

М. В. Качинский, Е. В. Листопад, А. А. Петровский, А. В. Станкевич
Кафедра электронных вычислительных средств, Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: listopad88@gmail.com, {palex, stankevich, kachinsky}@bsuir.by

Приводится краткий обзор рынка современных FPGA-кластеров. Рассматриваются технические характеристики и особенности использования платформы РУПК-50 производства ООО «НИЦ СЭ и НК» (г. Таганрог, РФ). Описываются варианты аппаратных реализаций алгоритма криптографического хэширования SHA-1 на одном FPGA-кристалле. Приводится оценка производительности вычислительной системы алгоритма SHA-1, построенной на базе РУПК-50.

Введение

Актуальность использования современных FPGA-кластеров (реконфигурируемых вычислительных платформ, построенных на базе нескольких идентичных FPGA-кристаллов) при построении высокопроизводительных цифровых устройств связана со стремлением специалистов выполнить аппаратные реализации весьма трудоемких с вычислительной точки зрения задач, которые на данный момент не представляется возможным реализовать на базе одного FPGA-кристалла. Появление FPGA-кластеров дало возможность разработчикам решать комплексные задачи, разбивая их при этом на несколько функциональных блоков, и реализуя каждый из них на отдельном кристалле; а также эффективно реализовывать распараллеливание вычислений: внутри кристалла — путем размещения нескольких идентичных IP-ядер, и на межкристальном уровне — путем построения собственного внутрисистемного интерфейса FPGA-кластера.

I. Обзор рынка платформ

В настоящий момент на зарубежном рынке представлено большое количество многокристальных аппаратных платформ на базе FPGA [1] от различных фирм-производителей, таких как COPACOBANA (Германия), Picocomputing (США), SciEngines (Германия), Dini Group (США). В России разработкой многокристальных реконфигурируемых вычислительных средств занимается ООО «Научно-исследовательский центр супер-ЭВМ и нейрокомпьютеров» («НИЦ СЭ и НК»). На базе его разработок строятся реконфигурируемые вычислительные системы, которые успешно применяются для решения задач цифровой обработки сигналов.[2] У данного производителя имеется множество реализаций аппаратных платформ, таких как РУПК-25, РУПК-50, «Ригель», «Тайгета», «Атлас» и др. на базе FPGA современных семейств фирмы Xilinx различного исполнения, а также всё необходимое разработчику системное и прикладное программное обеспечение.

II. Платформа РУПК-50

Исследования проводились для аппаратной платформы РУПК-50 (см. рис. 1), которая классифицируется производителем как ускоритель персонального компьютера (ПК), и предназначена для наращивания возможностей ПК при решении следующих задач:

- математическое моделирование сложных технических и природных процессов;
- символьная обработка информации;
- оптимизация эксплуатации нефтяных месторождений;
- цифровая обработка сигналов;
- криптография.

Рис. 1 – Платформа РУПК-50

РУПК-50 построен на основе базового модуля 16V5-50, который состоит из 16 вычислительных ПЛИС XC5VLX110-1FFG1153C и одной интерфейсной ПЛИС XC5VLX50T-1FFG1136C, имеет тактовую частоту 200 МГц, заявленную производительность 50 Гфлопс и внешний интерфейс Gigabit Ethernet. Вычислительный ресурс базового модуля представляет собой поле из 16 идентичных ПЛИС, на основе которых пользователь имеет возможность создавать любые вычислительные структуры. Для эффективного использования РУПК-50 при построении вычислительной системы был разработан кольцевой внутрисистемный интерфейс, позволяющий пользователю осуществлять обмен данными с каждой вычислительной ПЛИС базового модуля платформы.

III. Реализации процессоров

В ходе исследований преследовалась цель построить вычислительную систему на базе РУПК-50, использовав реализации процессоров алгоритма криптографического хэширования SHA-1 [3], имеющие максимально высокую производительность и обеспечивающие оптимальное использование вычислительных ресурсов кристаллов аппаратной платформы. В связи с этим максимально эффективным усматривалось решение по использованию процессоров, реализованных на конвейерных схемах [4]. В ходе исследований вопросов размещения таких процессоров на кристалле РУПК-50 (Xilinx XC5VLX110) было построено 3 тестовых специализированных процессора, технические характеристики которых приведены в таблице 1. Следует отметить, что для экспериментов строились специализированные процессоры с обработкой входного сообщения длиной не более 160 бит (20 символов в кодировке ASCII).

Таблица 1 – Характеристики процессоров

№	Кол-во ступеней конвейера	Ресурсы FPGA (Slices)	Производительность, (Гбит/с)	Частота, МГц
1.	82	6869(39%)	93.98	197.083
2.	83	7547(43%)	176.211	176.211
3.	162	8215(47%)	105.01	220.213

Первый вариант процессора подразумевает использование 82-ступенчатой конвейерной схемы, в которой одна ступень используется для фиксации исходных данных во входных регистрах, восемьдесят ступеней используются для вычисления всех восьмидесяти итераций алгоритма (при этом одна ступень конвейера вычисляет одну итерацию), и одна ступень используется для фиксации результата в выходном регистре процессора.

Второй вариант процессора подразумевает использование той же конвейерной схемы, однако с другой структурой вычислительных блоков внутри конвейера. В частности, модифицированных вычислительных блоков требуется использовать 79 вместо 80, и необходимы дополнительные включения в структуру конвейера блоков предварительных и финальных вычислений. Таким образом, конвейерный блок обработки будет иметь 81 ступень, а сама конвейерная схема процессора будет 83-ступенчатой (за счет использования входных и выходных регистров).

Третий вариант процессора подразумевает использование 162-ступенчатой конвейерной схемы. Такая схема отличается от 82-ступенчатой схемы использованием в своем составе расширенного конвейерного блока обработки, в котором одна итерация алгоритма вычисляется на двух ступенях конвейера.

Для каждого из рассмотренных вариантов процессоров было разработано VHDL описание и выполнен синтез для FPGA-кристалла XC5VLX110.

IV. Построение вычислительной системы

Теоретически все описанные варианты реализованных процессоров позволяют разместить по 2 идентичных вычислительных ядра на каждом кристалле платформы. Однако, анализируя рассмотренные варианты и выполняя оценку их характеристик, следует отметить следующее. Второй вариант процессора имеет худшие показатели производительности при значительных аппаратных затратах ресурсов FPGA, и не может рассматриваться в качестве оптимального кандидата на использование при построении FPGA-кластера. Третий вариант процессора имеет лучшие показатели производительности, однако при размещении двух его ядер на кристалле показатель аппаратных затрат ресурсов FPGA достигает значения в 94% (без учета ресурсов внутрисистемного интерфейса кристалла). Это в свою очередь не позволяет САПР Xilinx ISE выполнить эффективное размещение и трассировку элементов на кристалле без значительного снижения показателя тактовой частоты (а соответственно и производительности системы). Первый вариант процессора является наиболее оптимальным и позволяет построить на базе РУПК-50 специализированный FPGA-кластер со следующими характеристиками.

Таблица 2 – Характеристики FPGA-кластера

Платформа	РУПК-50
Кол-во ядер на кристалле, шт	2
Кол-во ядер на платформе, шт	32
Полученная частота, МГц	190
Производительность системы, Гбит/с	2899,28

В качестве сферы применения исследуемых FPGA-кластеров стоит рассматривать сферу защиты информации, в частности такие ее элементы как «идентификация пользователя» и «верификация целостности данных».

1. Международная научно-техническая конференция, приуроченная к 50-летию МРТИ–БГУИР : материалы конф. В 2 ч. Ч. 1 / редкол. : А. А. Кураев [и др.]. – Минск : БГУИР, 2014. – С. 306–307.
2. Международная конференция "Цифровая обработка сигналов и её применение – DSPA-2012": материалы конф. / редкол. : – Москва, 2012. – С. 377–381.
3. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер // Издательство: Триумф, 2012. – 815 с.
4. Mohamed KhaJil Hani, Ahmad Zoo Sha'ameri, Chong Wei Sheng. Pipeline Implementation of Secure Hash Algorithm (SHA-l) [Электронный ресурс]. – 2000. – Режим доступа:http://eprints.utm.my/10992/1/MohamedKhalilHani2000_PipelineImplementationofSecureHash.pdf – Дата доступа: 25.06.2015.