УДК 004.75:004.272

КОНВЕЙЕРНЫЙ ПРОЦЕССОР АЛГОРИТМА ХЭШИРОВАНИЯ MD5 НА БАЗЕ FPGA

В.Ю. ГЕРАСИМОВИЧ[1], М.В. КАЧИНСКИЙ[2], А.В. СТАНКЕВИЧ[3]

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
[1]gerasimovich@bsuir.by, [2]kachinsky@bsuir.by, [3]stankevich@bsuir.by

Рассматривается аппаратная реализация алгоритма хэширования MD5 на базе field-programmable gate array (FPGA) для приложений, требующих высокой производительности. Проведен анализ возможных архитектурных решений специализированного процессора, приведены характеристики разработанных процессоров.

Ключевые слова: алгоритм хэширования MD5, специализированный процессор, FPGA.

Алгоритм хэширования MD5 применяется для создания хэша (дайджеста) фиксированной длины 128 бит для сообщений произвольной длины [1]. Обычно полученный хэш используется с целью последующей проверки отсутствия искажений исходного сообщения. Несмотря на известные недостатки [2], алгоритм MD5 широко используется в различном программном обеспечении для идентификации блоков данных или целостности файлов, для хэширования паролей.

Программная реализация алгоритма MD5 обладает сравнительно невысокой производительностью, недостаточной для высокопроизводительных приложений. Поскольку алгоритм MD5 имеет последовательную природу, то при аппаратной реализации возможности параллельного выполнения операций ограничены имеющимися в алгоритме зависимостями по данным. Возможны следующие архитектурные варианты аппаратной реализации алгоритма MD5 [3, 4]:

- итеративная архитектура;
- конвейерная архитектура на уровне раундов;
- полностью конвейерная (развернутая) архитектура.

В итеративной архитектуре используется только один блок обработки, реализующий шаг алгоритма MD5. Для вычисления хэша данные подаются на блок обработки в цикле 64 раза, в результате чего финальное значение дайджеста получается за 66 тактов (два такта используются для приема исходного MD5 блока и выдачи хэша). Данная архитектура обеспечивает минимальное использование ресурсов FPGA, однако, и минимальное быстродействие.

Наиболее высокой производительностью обладают аппаратные реализации алгоритма MD5 на базе FPGA, позволяющие организовать конвейерный вычислительный процесс. В докладе проводится анализ возможных архитектурных решений конвейерного процессора алгоритма MD5, позволяющих получить различную производительность при различных аппаратных затратах. Приводятся характеристики разработанных процессоров для кристалла FPGA семейства Virtex 5.

В конвейерной архитектуре на уровне раундов используется независимость по данным между раундами алгоритма. В этом случае, конвейер содержит 4 ступени по одной на каждый раунд алгоритма. 16 шагов каждого раунда выполняются итеративно в блоке обработки соответствующей ступени конвейера. В таком процессоре одновременно вычисляются хэши 4 входных сообщений, причем первый хэш получается через 76 тактов, а последующие – каждые 19 тактов.

Библиотека БГУИР

В полностью конвейерной архитектуре используется 64 блока обработки по одному на каждый шаг алгоритма MD5. Данный вариант процессора MD5 содержит конвейерный блок обработки из 65 ступеней: 64 ступени – непосредственно шаги алгоритма хэширования, 1 ступень – для расчета предварительного операнда для первого шага алгоритма. В результате цикл вычисления хэша разворачивается во времени, образуя конвейерную (поточную) структуру. В такой структуре одновременно вычисляются хэши 64 входных сообщений, причем первый хэш получается через 65 тактов, а последующие – в каждом такте. Полностью конвейерная (развернутая) архитектура обеспечивает в установившемся режиме высокую скорость вычисления хэша за счет использования дополнительных ресурсов FPGA.

Дополнительное повышение производительности конвейерного процессора можно получить за счет разделения одного шага алгоритма MD5 на несколько ступеней конвейера. Такая возможность связана с наличием на одном шаге алгоритма последовательности логических и арифметических операций. При реализации одного шага алгоритма на двух ступенях конвейера число ступеней увеличится на 64 и будет равно 129. Увеличение числа ступеней позволяет уменьшить количество уровней логики в ступени процессора для реализации вычислительных операций, что уменьшает критический путь и увеличивает пропускную способность процессора.

В табл. 1 приведены характеристики разработанных процессоров для кристалла FPGA xc5vlx110-1ff1153 для случая длины входного сообщения менее размера одного блока данных алгоритма MD5 (512 бит). Для аппаратных затрат в скобках приведен процент от доступных ресурсов кристалла.

Табл. 1. Аппаратные затраты и производительность различных вариантов конвейерного процессора алгоритма хэширования MD5 на базе FPGA xc5vlx110-1ff1153

Характеристика	Вариант конвейерного процессора		
	Конвейер на уровне раундов	Конвейер с 65 ступенями	Конвейер с 129 ступенями
Триггеры	2341 (3%)	9090 (13%)	14967 (21%)
Просмотровые таблицы (LUT)	2069 (2%)	7033 (10%)	10445 (15%)
Секции (slice)	801 (4%)	2812 (16%)	4055 (23%)
Тактовая частота, МГц	167	199	325
Пропускная способность, Гбит/с	4,5	101,9	166,4

По приведенным в табл. 1 данным можно выбрать реализацию конвейерного процессора алгоритма хэширования MD5 для требуемой производительности и аппаратным затратам в зависимости от решаемой задачи.

Список литературы

1. *Rivest, R.L.,* The MD5 Message-Digest Algorithm // RFC-1321. 1992. MIT Laboratory for Computer Science and RSA Data Security, Inc.

2. CERT Vulnerability Note VU#836068. [Электронный ресурс]. – Режим доступа: http://www.kb.cert.org/vuls/id/836068. - Дата доступа: 9.08.2010.

3. *Wang Y, Zhao Q, Jiang L, Yi S.* Ultra high throughput implementations for MD5 hash algorithm on FPGA // High Performance Computing and Applications. 2010. Volume 5938, P. 433-441.

4. *Zhijie Shi, Chujiao Ma, Jordan Cote, Bing Wang,* Hardware Implementation of Hash Functions // Introduction to Hardware Security and Trust. 2012. Springer. P. 427.

Библиотека БГУИР