КОНВЕЙЕРНЫЙ ПРОЦЕССОР ХЭШ-ФУНКЦИИ SHA-256

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

Рассматривается аппаратная реализация хэш-функции SHA-256 для встраиваемых систем с высокой производительностью. Предлагаемый специализированный процессор SHA-256 имеет конвейерную архитектуру. Приводятся характеристики реализации на базе кристалла ПЛИС XC7VX485T-2FFG1761 фирмы Xilinx.

Хэш-функция SHA-256 [1] относится к семейству SHA-2. Алгоритм SHA-256 практически используется в разнообразных криптографических приложениях. Для приложений, требующих высокой производительности (например, майнеры криптовалют), необходима аппаратная реализация алгоритма. В докладе рассматривается конвейерная реализация алгоритма SHA-256.

Алгоритм вычисления хэш-функции обеспечивает сжатие входного сообщения (для сообщений длиной менее 256 бит – расширение) и получение хэш-значения фиксированной длины 256 бит. Алгоритм заключается в выполнении 64 однотипных циклов (раундов). На рис. 1 приведена схема вычислений для одного раунда.

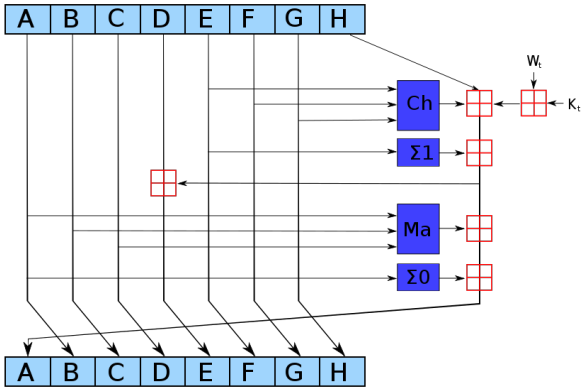

Рис. 1 – Схема вычислений для одного раунда алгоритма SHA-256

На первом раунде 32-разрядные переменные A-H инициализируются константами алгоритма [1]. Входными значениями переменных A-H для следующего раунда являются выходные значения переменных A-H предыдущего, поэтому раунды нельзя вычислять параллельно. Kt является раундовой константой, Wt – раундовым входным словом [1].

В конвейерной архитектуре (рис. 2) блоком данных, продвигающимся по конвейеру является состояние, получаемое на выходе предыдущего процессорного ядра. Каждое процессорное ядро выполняет один раунд алгоритма SHA-256, и эти ядра включены последовательно. Вектор инициализации (IV) подается на вход первого процессорного ядра. Для реализации 64 раундов алгоритма используется цепочка из 64 последовательно включенных процессорных ядер. Параллельно с продвижением текущего состояния по конвейеру продвигается входной блок и текущие данные экспандера для формирования требуемого значения Wt для соответствующего процессорного ядра.

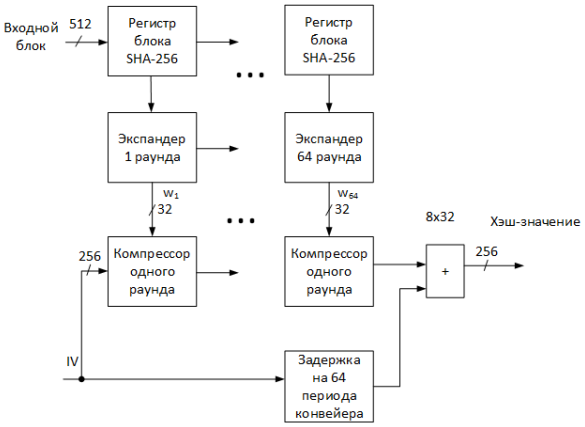

Рис. 2 – Конвейерная архитектура специализированного процессора SHA-256

Выходные данные 64-го процессорного ядра складываются с задержанным на 64 периода (цикла) работы конвейера значением IV для получения выходного хэш-значения.

Если на конвейерный процессор каждый цикл работы конвейера подавать новый входной блок и новый вектор инициализации (в случае, если сообщение занимает более одного блока SHA-256), то по истечении 64 циклов (латентность конвейера) на выходе в каждом цикле работы конвейера будет появляться новое хэш-значение. Если цикл конвейера будет равен одному такту работы вычислительной системы, то производительность конвейерного процессора будет численно равна тактовой частоте. Значение тактовой частоты будет соответствовать числу вычисляемых хэш-значений в секунду.

При конвейерной реализации вычислений одного раунда необходимо принять меры для уменьшения непрерывной цепочки сложений (рис. 1), которая будет определять критический

путь. Для этого следует учесть некоторые особенности алгоритма SHA-256: значения переменных B,C,D после выполнения текущего раунда совпадают со значениями переменных A,B,C до выполнения раунда, а значения переменных F,G,H – совпадают со значениями переменных E,F,G. Эту особенность можно проследить и на несколько раундов назад. Такая особенность алгоритма позволяет выполнить часть вычислений, использующих указанные переменные не в текущем, а в предыдущем такте, либо еще на такт раньше. Также можно формировать значение Wt не в текущем такте, а на такт или два раньше для синхронизации с вычислением новых значений переменных A и E.

Еще одна особенность алгоритма связана с возможностью разнесения на разные такты вычисления переменных E и A, поскольку при вычислении A частично используются промежуточные вычисления для E.

Конвейерная реализация выполнена с учетом указанных особенностей.

На первой ступени конвейера компрессора организуются предварительные вычисления сумм Wt+Kt+H и Wt+Kt+H+D, вторая ступень дополнительно вычисляет значение E и значение переменной $T1 = H + BSIG1(E) + CH(E,F,G) + Kt + Wt$ [1] для вычисления A на следующей ступени. Третья ступень является первой полной ступенью конвейера и она дополнительно к указанным выше действиям вычисляет значение A. Таким образом на полной ступени конвейера происходит вычисление значения переменной A текущего раунда и значения переменной E для следующего раунда.

На предпоследней ступени конвейера вычисляется значение A для последнего 64 раунда алгоритма. На последней ступени происходит сложение со значением вектора инициализации алгоритма. С учетом предварительных вычислений и завершающего сложения полный конвейер имеет 67 ступеней и спустя 67 тактов на его выходе появится первое хэш-значение. Далее конвейер будет каждый такт формировать новое хэш-значение при соответствующих изменениях входных данных.

Для разных ступеней конвейера компрессора с помощью конвейера экспандера формируются значения Wt. Для первых 16 раундов (раунды 1 - 16) экспандер реализует задержку входного блока SHA-256 и в качестве Wt выдает соответствующее 32-разрядное слово входного блока. Одна ступень конвейера экспандера для раундов 17-56 дополнительно содержит средства для расширения входного сообщения и вычисления Wt в соответствии с [1]. При реализации конвейера экспандера для раундов с 57 по 64 учтено то обстоятельство, что не все элементы входного блока данных будут использованы при вычислениях текущего значения Wt.

Аппаратные затраты конвейерного процессора SHA-256 после процедуры синтеза средствами ISE 14.7 для кристалла FPGA XC7VX485T-2FFG1761 приведены на рис. 3. По отчету средств синтеза максимальная тактовая частота составляет 323 МГц.

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	27478	607200	4%
Number of Slice LUTs	35160	303600	11%
Number of fully used LUT-FF pairs	15936	46702	34%
Number of bonded IOBs	1028	700	146%
Number of BUFG/BUFGCTRLs	1	32	3%

Рис. 3 – Аппаратные затраты предлагаемого конвейерного процессора SHA-256 после процедуры синтеза для кристалла FPGA XC7VX485T-2FFG1761

Для сравнения с предлагаемым процессором была выполнена реализация конвейерного ядра SHA-256 свободно распространяемого проекта Bitcoin–майнера [2] на таком же кристалле FPGA XC7VX485T-2FFG1761. Аппаратные затраты этого конвейерного процессора после процедуры синтеза приведены на рис. 4. По отчету средств синтеза Xilinx ISE 14.7 максимальная тактовая частота составляет 178 МГц.

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slice Registers	88419	607200	14%
Number of Slice LUTs	61058	303600	20%
Number of fully used LUT-FF pairs	12256	137221	8%
Number of bonded IOBs	3	700	0%
Number of BUFG/BUFGCTRLs	1	32	3%
Number of DCM_ADVs	1	0	

Рис. 4 – Аппаратные затраты конвейерного процессора SHA-256 [2] после процедуры синтеза для кристалла FPGA XC7VX485T-2FFG1761

По сравнению с свободно распространяемым проектом Bitcoin–майнера [2] предлагаемая реализация SHA-256 почти в два раза производительнее и требует примерно в два раза меньше аппаратных ресурсов кристалла FPGA.

Применительно к процессу майнинга криптовалют можно провести дополнительную минимизацию аппаратных затрат процессора за счет учета структуры заголовков блоков криптовалют.

1. National Institute of Standards and Technology (NIST), FIPS Publication 180-3: Secure Hash Standard, October 2008 [Электронный ресурс] – Режим доступа: https://csrc.nist.gov/publications/detail/fips/180/3/archive/2008-10-31. – Дата доступа: 18.09.2018.
2. Bitcoin-miner – [Электронный ресурс]. – Режим доступа: https://github.com/fpgaminer/Open-Source-FPGA-Bitcoin-Miner/tree/master/projectst. – Дата доступа: 18.09.2018.