УДК 004.0315 DOI: 10.18698/2541-8009-2023-6-860

ВЫЧИСЛИТЕЛЬ ХЕШ-ФУНКЦИИ SHA-256

С.В. Астахов fzastahov@gmail.com
Д.И. Вариханов denis.varihanov@ya.ru

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

В данной статье описывается разработка проекта устройства, производящего расчет внутреннего цикла алгоритма хеширования SHA-256. Устройство рассчитывает внутренний цикл алгоритма SHA-256 в соответствии со стандартом Secure Hash Standard. Хеш-функции, в том числе SHA-256, применяются главным образом для вычисления контрольных сумм, работы с электронной подписью и построения уникальных идентификаторов для наборов данных. Широкое применение хеш-функций в современных информационных системах обуславливает актуальность работы. При проектировании решены следующие задачи: анализ объекта разработки на функциональном уровне, разработка функциональной схемы устройства, описание устройства на языке Verilog, синтез RTL-схемы устройства.

Ключевые слова

SHA-256, хеш-функция, ПЛИС, FPGA, вычислитель, Verilog, Xilinx, цифровая схемотехника.

Введение. Несмотря на то, что хеш-функции легко могут быть реализованы программным путем, зачастую необходимо применять их для большого количества сообщений (например, при работе с блокчейном), в этих условиях разница в производительности программной и аппаратной реализации становится принципиальной (в пользу последней) [1].

В рамках данной статьи рассмотрена аппаратная реализация вычислителя, осуществляющего вычисление одной из самых широко применяемых хеш-функций —

SHA-256. Эта хеш-функция входит в состав семейства хеш-функций SHA-2, разработанных Агентством национальной безопасности США и опубликованных Национальным институтом стандартов и технологий в федеральном стандарте обработки информации FIPS PUB 180-2 [2].

Алгоритм расчета SHA-256. Все хеш-функции семейства SHA-2 построены на основе структуры Меркла-Дамгора, предусматривающей разбиение входных сообщений произвольной длины на блоки фиксированной длины и работающей с ними по очереди с помощью функции сжатия, каждый раз принимая входной блок с выходным от предыдущего прохода [3].

В случае SHA-256 каждое сообщение разбивается на блоки по 16 32-битных слов, алгоритм пропускает каждый блок сообщения через цикл с 64 итерациями. В разработанном устройстве производится преобразование сообщения в рамках этих 64 циклов, разбиение исходного сообщения на блоки возлагается на другое (внешнее) цифровое устройство или стороннюю программу.

Схема одной итерации алгоритма представлена на рисунке 1, на ней:

- A, B, C, D, E, F, G, H — служебные переменные;
- Ch, Σ1, Ma, Σ0 — математические функции, описанные в FIPS PUB 180-2 и RFC 4634 [4];
- t — номер итерации;
- K_t — служебная константа;
- W_t — слово из блока сообщения.

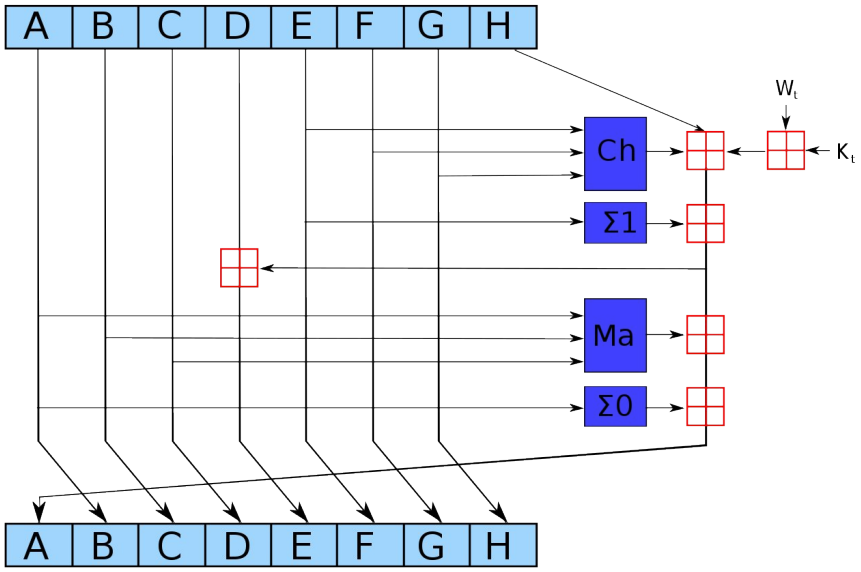

Рис. 1. Схема одной итерации алгоритма SHA-256

Разработка функциональной схемы устройства. При анализе предметной области, было заключено, что устройство должно состоять из блока управления, блока памяти переменных, блока памяти констант, выходного буфера, мультиплексирующего блока и вычислительного блока. Функциональная схема вычислителя представлена на рисунке 2.

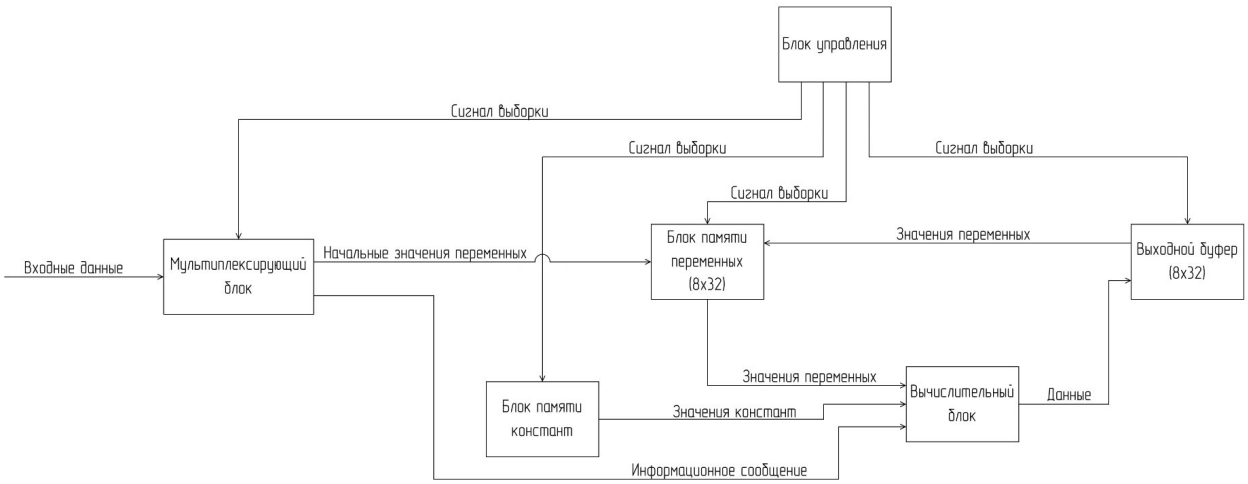

Рис. 2. Функциональная схема вычислителя

Блок памяти переменных каждые 64 цикла исполнения алгоритма инициализируется извне, в остальных циклах он сохраняет значения полученные в предыдущем цикле. Поэтому данный блок должен иметь два информационных входа для соответствующих целей.

Мультиплексирующий блок в начале каждого раунда шифрования перенаправляет значения служебных переменных с информационного входа схемы в память. После этого данных блок перенаправляет значения информационных сообщений на вход вычислительного блока.

Вычислительный блок принимает на вход значения переменных из блока памяти переменных, значение очередной служебной константы и фрагмент информационного сообщения. Данные блок отвечает непосредственно за расчеты, описанные в стандарте SHA-256.

Выходной буфер принимает значения, полученные в ходе вычислений и передает их на выход устройства, а также в блок памяти переменных [5].

Блок памяти констант представляет из себя постоянную память, хранящую 64 служебных константы, которые необходимы для расчетов.

Блок управления на основе тактирующего сигнала генерирует необходимые сигналы выборки для блоков памяти, так как из-за большой разрядности все они имеют внутри себя схему выборки и для операций ввода-вывода используют мультиплексирование с разделением по времени.

Разработка блока вычислений. Блок вычислений представляет из себя набор модулей, вычисляющих значения функций Ch, Σ1, Ma, Σ0, является комбинационной схемой [6]. В качестве примера рассмотрим модуль, вычисляющий функцию Σ0. Функция задается формулой:

$$\Sigma 0 = (a\ rotr\ 2)\ xor\ (a\ rotr\ 13)\ xor\ (a\ rotr\ 22)$$

Код на языке Verilog, реализующий данные вычисления приведен в листинге 1.

Листинг 1 — исходны код модуля сигма-0

```
// подключение описания функции цикл. сдвига вправо (rotr)
`include "right_cyclic_shift.v"
module func_sigma0(in_A, func);

     input wire[31:0] in_A;                // список входов
     output wire[31:0] func;               // список выходов

     wire[31:0] A2, A13, A22;              // список соединений

     right_cyclic_shift #(2)
     A2_node( .out (A2), .num (in_A));     // A2 := A rotr 2

     right_cyclic_shift #(13)
     A13_node( .out (A13), .num (in_A));   // A13 := A rotr 13

     right_cyclic_shift #(22)
     A22_node( .out (A22), .num (in_A));   // A22 := A rotr 22

     // выход := A2 xor A13 xor A22
     assign func = A2 ^ A13 ^ A22;
endmodule
```

RTL-схема данного модуля, сгенерированная Xilinx ISE на основе приведенного кода, показана на рисунке 3 [7].

Аналогично тому, как к модулю сигма-0 был подключен модуль циклического сдвига вправо, модули вычисления функций Ch, Σ1, Ma, Σ0 были подключены к главному модулю блока вычислений.

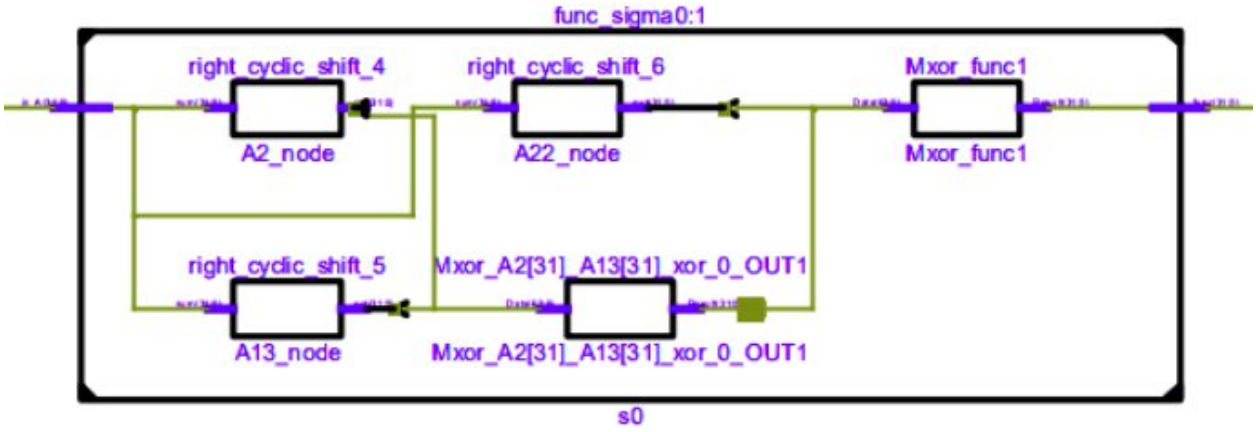

Рис. 3. RTL-схема модуля Сигма-0

Тестирование блока вычислений. В результате тестирования блока вычислений была получена временная диаграмма, представленная на рисунке 4 [8]. В нижней половине диаграммы представлены входные значения, в верхней — выходные.

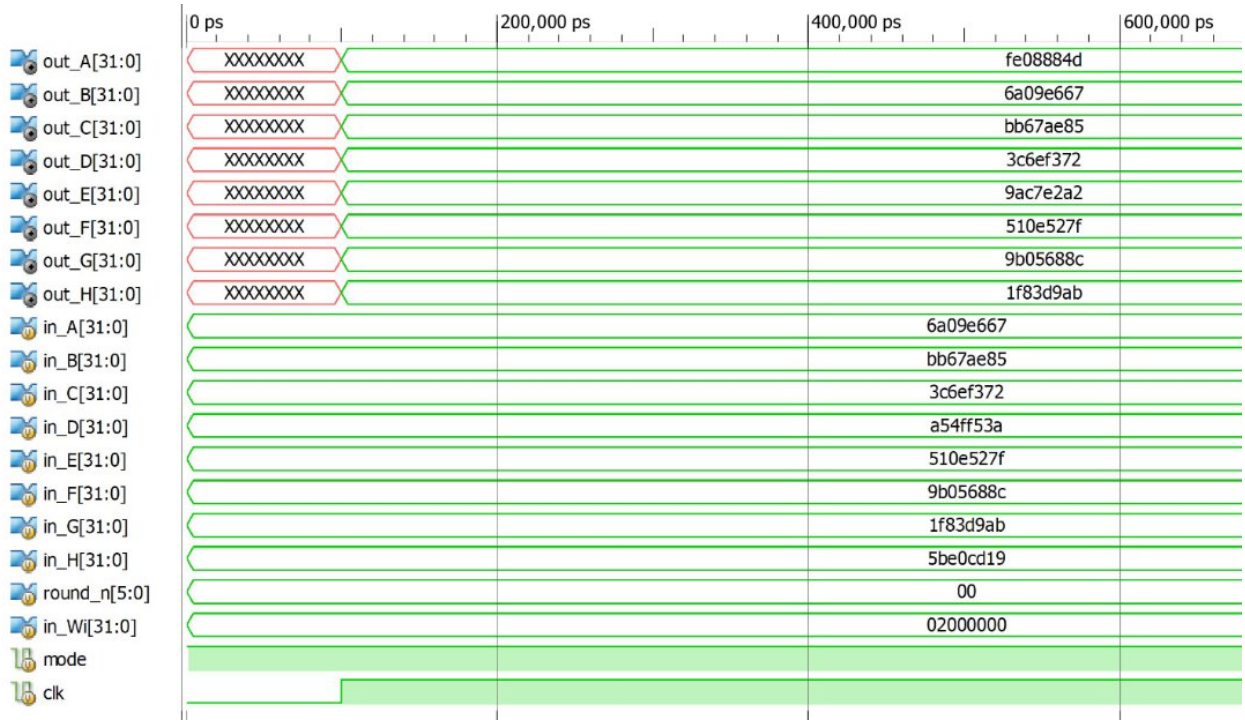

Рис. 6. Временная диаграмма работы блока вычислений

С целью проверки полученных результатов, вычисление результатов выполнения одного раунда SHA-256 было повторно проведено вручную с теми же начальными значениями [9]. Полученные двумя способами результаты совпали, следовательно, тестирование прошло успешно.

Соединение основных блоков. После разработки блока вычислений были спроектированы блок памяти переменных, блок памяти констант, выходной буфер, мультиплексирующий блок. Их внутреннее устройство довольно тривиально, а общие принципы работы очевидны из функциональной схемы. Блок памяти переменных и выходной буфер являются последовательными схемами на базе 32-

битных регистров, они мультиплексируют ввод-вывод во времени, что позволяет взаимодействовать с устройством по 32-битной шине данных [10].

RTL-схема выходного буфера показана на рисунке 7, в ее правой части находятся регистры, в левой — схема управления записью.

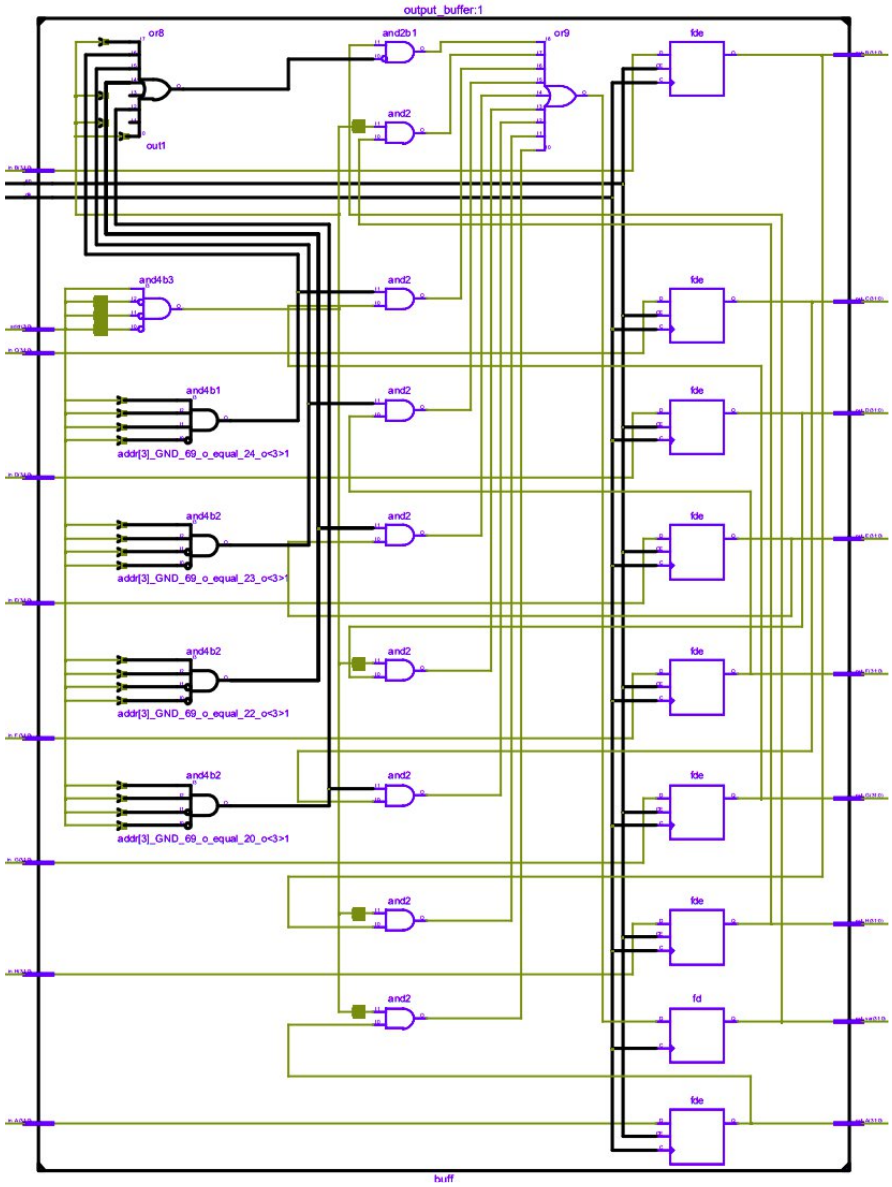

Рис. 7. RTL-схема выходного буфера

Временная диаграмма работы основных блоков устройства представлена на рисунке 8.

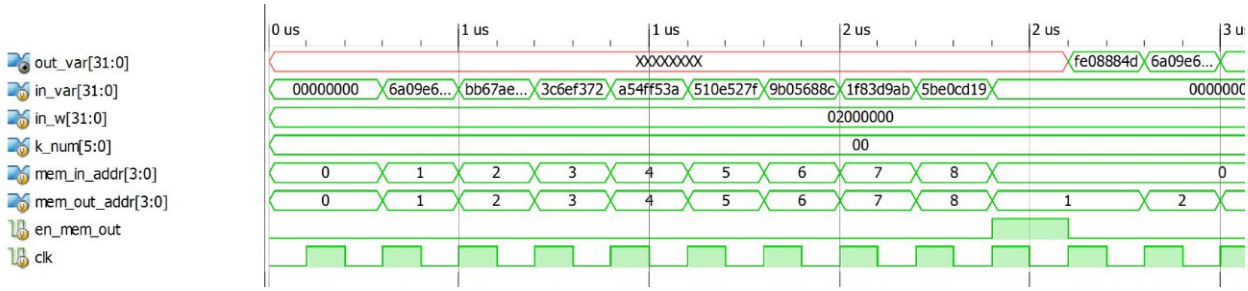

Рис. 8. Временная диаграмма работы основных блоков устройства

Для проверки основных блоков устройства использованы те же значения, что и для проверки блока вычислений, однако теперь значения подаются на вход (вторая строка временной диаграммы) и выход (первая строка временной диаграммы) с мультиплексированием по времени.

Блок управления. Так как сочетания сигналов выборки полностью определяются последовательным номером исполняемого цикла алгоритма SHA-256, для обеспечения корректной работы блоков памяти и упрощения внешнего интерфейса устройства был разработан блок управления.

Временная диаграмма работы блока управления приведена на рисунке 9.

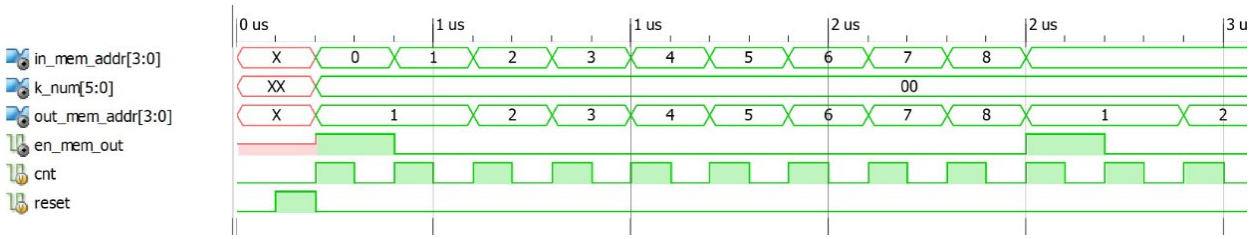

Рис. 9. Временная диаграмма работы блока управления

Этот блок на основе тактового сигнала изменяет значение внутреннего счетчика. На основе значения внутреннего счетчика генерируются управляющие сигналы, соответствующие входным сигналам на рисунке 8 (за исключением начального адреса выходного буфера, который не оказывает влияния на корректность работы устройства).

Заключение. В рамках представленной статьи был рассмотрен процесс проектирования вычислителя хеш-функции SHA-256. Была составлена функциональная схема устройства, исходя из которой вычислитель был представлен в виде совокупности блоков: блока управления, блока памяти переменных, блока памяти констант, выходного буфера, мультиплексирующего блока и вычислительного блока. Выборочно были приведены примеры исходного кода описания некоторых блоков вычислителя и их RTL-схемы. Проведена проверка работоспособности ключевых блоков устройства посредством моделирования временных диаграмм их работы.

Литература

[1] Y. Hashimoto, S. Noda, - Pricing of Mining ASIC and Its Implication to the High Volatility of Cryptocurrency Prices / Y. Hashimoto, S. Noda // Social Science Research Network : электронный журнал. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3368286. – Дата публикации: 08.04.2019.

[2] Quynh H. Dang, Secure Hash Standard (SHS) // Quynh H. Dang – Gaithersburg : National Institute of Standards and Technology, 2015. – 36 p.

[3] Семашко А.В., Кулаков А.В. Криптографическая хеш-функция // Информационные системы и технологии. - Нижний Новгород: 2018. - С. 534-538.

[4] D. Eastlake. RFC 4634, US Secure Hash Algorithms // D. Eastlake – New Jersey : AT&T Labs, 2006. – 108 c.

[5] Попов А.Ю. Проектирование цифровых устройств с использованием ПЛИС. – М.: изд-во МГТУ, 2009. – 79 с.

[6] Уилкинсон Б. Основы проектирования цифровых схем / Б. Уилкинсон. – М.: Издательский дом "Вильямс", 2004. – 320 с. – ISBN 5-8459-0685-7.

[7] J. Cong, B. Liu, S. Neuendorffer, J. Noguera, K. Vissers and Z. Zhang. High-Level Synthesis for FPGAs: From Prototyping to Deployment / J. Cong, B. Liu, S. Neuendorffer, J. Noguera, K. Vissers and Z. Zhang // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems : электронный журнал. – URL: https://ieeexplore.ieee.org/abstract/document/5737854 – Дата публикации: 22.04.2011.

[8] C. Spear. System Verilog for verification. C. Spear. - Marlboro: Springer Science, 2008/ — 425 p. — ISBN 978-0-387-76529-7.

[9] Разбираем каждый шаг хэш-алгоритма SHA-256 // habr : сайт. – URL: https://habr.com/ru/companies/selectel/articles/530262/ (дата обращения: 16.06.2023)

[10] Патент № 2526370, Российская Федерация, H04J 3/16. Устройство и способ передачи множества информационных сигналов с разделенным по времени мультиплексированием : № 2011137841/07 : заявл. 12.03.2010 : опубл. 20.08.2014 / Форстер К., Мулл А., Доехла С., Герхаузер Х., Хеубергер А. – 28 с.

Астахов Сергей Викторович — бакалавр кафедры «Компьютерные системы и сети», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Вариханов Денис Игоревич — бакалавр кафедры «Компьютерные системы и сети», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Научный руководитель — Ким Тамара Александровна, ассистент кафедры «Компьютерные системы и сети», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:

Астахов С.В., Вариханов Д.И. Вычислитель хеш-функции SHA-256. *Политехнический молодежный журнал*, 2023, № 07 (83). http://dx.doi.org/10.18698/2541-8009-2023-6-865

SHA-256 HASH FUNCTION CALCULATOR

S.V. Astakhov fzastahov@gmail.com
D.I. Varikhanov denis.varihanov@ya.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

This article describes the development of a device design that calculates the internal cycle of the SHA-256 hashing algorithm. The device calculates the internal cycle of the SHA-256 algorithm in accordance with the Secure Hash Standard. Hash functions, including SHA-256, are mainly used to calculate checksums, work with electronic signatures and build unique identifiers for data sets. The widespread use of hash functions in modern information systems determines the relevance of the work. When designing, the following tasks were solved: analysis of the development object at the functional level, development of the functional scheme of the device, description of the device in Verilog, synthesis of the RTL scheme of the device.

Keywords

SHA-256, hash function, FPGA, computer, calculator, Verilog, Xilinx, digital circuitry.

References

[1] Y. Hashimoto, S. Noda, - Pricing of Mining ASIC and Its Implication to the High Volatility of Cryptocurrency Prices / Y. Hashimoto, S. Noda // Social Science Research Network : electronic journal. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3368286. – published: 08.04.2019.

[2] Quynh H. Dang, Secure Hash Standard (SHS) // Quynh H. Dang – Gaithersburg : National Institute of Standards and Technology, 2015. – 36 p.

[3] Semashko A.V., Kulakov A.V. Kriptograficheskaya hesh-funkciya. Informacionnye sistemy i tekhnologii // Informacionnye sistemy i tekhnologii [Cryptographic hash function. Information systems and technologies // Information systems and technologies]. - Nizhny Novgorod: 2018. - pp. 534-538. (In Russ.).

[4] D. Eastlake. RFC 4634, US Secure Hash Algorithms // D. Eastlake – New Jersey : AT&T Labs, 2006. – 108 c.

[5] Popov A.Y. Proektirovanie cifrovyh ustrojstv s ispol'zovaniem PLIS [Design of digital devices using FPGAs]. – M.: publishing house of MSTU, 2009. - 79 p. (In Russ.).

[6] Wilkinson B. Osnovy proektirovaniya cifrovyh skhem [Fundamentals of digital circuit design] / B. Wilkinson. – M.: Williams Publishing House, 2004. – 320 p. – ISBN 5-8459-0685-7. (In Russ.).

[7] J. Cong, B. Liu, S. Neuendorffer, J. Noguera, K. Vissers and Z. Zhang. High-Level Synthesis for FPGAs: From Prototyping to Deployment / J. Cong, B. Liu, S. Neuendorffer, J. Noguera, K. Vissers and Z. Zhang // IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems : electronic journal. – URL: https://ieeexplore.ieee.org/abstract/document/5737854 – published: 22.04.2011.

[8] C. Spear. System Verilog for verification. C. Spear. - Marlboro: Springer Science, 2008/ — 425 p. — ISBN 978-0-387-76529-7.

[9] Razbiraem kazhdyj shag hesh-algoritma SHA-256 [Analyzing each step of the SHA-256 hash algorithm] // habr : website. – URL: https://habr.com/ru/companies/selectel/articles/530262 / (accessed: 06.16.2023) (In Russ.).

[10] Patent No. 2526370, Russian Federation, H04J 3/16. Ustrojstvo i sposob peredachi mnozhestva informacionnyh signalov s razdelennym po vremeni mul'tipleksirovaniem [Device and method of transmitting multiple information signals with time–separated multiplexing] : No. 2011137841/07 : application 12.03.2010 : publ. 20.08.2014 / Forster K., Mull A., Doehla S., Gerhauser H., Heuberger A. - 28 p. (In Russ.).

Astakhov S.V. — B.Sc. Student, Department of Computer Systems and Networks, Bauman Moscow State Technical University, Moscow, Russian Federation.

Varikhanov D.I. — B.Sc. Student, Department of Computer Systems and Networks, Bauman Moscow State Technical University, Moscow, Russian Federation.

Scientific advisor — Kim T.A., Assis. Professor, Department of Computer Systems and Networks, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:

Astakhov S.V., Varikhanov D.I. SHA-256 hash function calculator. *Politekhnicheskiy molodezhnyy zhurnal*, 2023, no. 06 (83). (In Russ.). http://dx.doi.org/10.18698/2541-8009-2023-6-865