ИНФОРМАТИКА

УДК 004.9:003.26
MSC 11T71

Пример внутренней функции для схемы SPONGE*

Р. М. Оспанов, Е. Н. Сейткулов, Н. М. Сисенов, Б. Б. Ергалиева

Евразийский национальный университет им. Л. Н. Гумилёва, Казахстан,
010000, Нур-Султан, ул. Сатпаева, 2

Для цитирования: *Оспанов Р. М., Сейткулов Е. Н., Сисенов Н. М., Ергалиева Б. Б.* Пример внутренней функции для схемы SPONGE // Вестник Санкт-Петербургского университета. Прикладная математика. Информатика. Процессы управления. 2021. Т. 17. Вып. 3. С. 287–293. https://doi.org/10.21638/11701/spbu10.2021.306

Предложен новый вариант внутренней функции, лежащей в основе перспективной современной схемы построения криптографических хеш-функций Sponge (криптографическая губка). Описываемый пример аналогичен перестановке Keccak, но имеет ряд основных отличий. Внутренняя функция оперирует над 2048-битовым состоянием S, который можно рассматривать как трехмерный битовый массив размером $4 \times 8 \times 64$. Структуру внутренней функции составляют 5 преобразований, аналогичных Keccak. Но, во-первых, в приведенном примере вместо 5-битового S-блока используется 8-битовый, в связи с чем изменены параметры трехмерного представления состояния. Во-вторых, для формирования раундовых констант вместо регистра сдвига с линейной обратной связью применяется словарный регистр сдвига с обратной связью по переносу кольцевой конфигурации. Проведен анализ свойств этих преобразований.

Ключевые слова: информационная безопасность, криптография, хеш-функция, модификация Sponge, симметричное шифрование.

1. Введение. В настоящее время существует множество различных схем для построения криптографических хеш-функций. Наиболее популярной и перспективной альтернативой стала схема Sponge (криптографическая губка) [1, 2]. Схема Sponge — это простая итерационная схема для построения функции с входом переменной длины и выходом произвольной длины на основе внутренней функции f, являющейся преобразованием фиксированной длины или перестановкой, оперирующей с постоянным числом b битов ($b = r + c$). Значение r называется битовой скоростью, а c — мощностью. В алгоритме используется переменная S длиной b, называемая состоянием. К состоянию S и применяют внутреннюю функцию f. С помощью этой схемы, кроме хеш-функций, можно создавать такие криптопримитивы как блочные симметричные

* Работа выполнена при финансовой поддержке Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (грант № AP06851124).

шифры, коды аутентификации сообщения и поточные шифры. По такой схеме был спроектирован алгоритм Keccak [3], ставший победителем конкурса SHA-3. В алгоритме Keccak внутренняя функция $f : Z_{2^b} \to Z_{2^b}$ представляет собой перестановку множества Z_{2^b}, построенную как итерационный блочный шифр, в котором раундовые ключи заменяются некоторыми простыми раундовыми константами.

В данной статье рассматривается пример внутренней функции, аналогичный перестановке Keccak, но имеющий некоторые отличия. Во-первых, вместо 5-битового S-блока используется 8-битовый. В связи с этим изменены параметры трехмерного представления состояния. Во-вторых, для формирования раундовых констант вместо регистра сдвига с линейной обратной связью применяется словарный регистр сдвига с обратной связью по переносу кольцевой конфигурации (известный в англоязычной литературе как «word ring Feedback with Carry Shift Register (word ring FCSR)»).

Регистры сдвига с обратной связью по переносу обладают хорошими свойствами регистров сдвига с линейной обратной связью: последовательностями с известным периодом и хорошими статистическими свойствами. Но в отличие от регистров сдвига с линейной обратной связью они обеспечивают внутреннюю устойчивость к алгебраическим и корреляционным атакам. Регистры сдвига с обратной связью по переносу кольцевой конфигурации обобщают предыдущие представления Галуа и Фибоначчи и имеют много преимуществ по сравнению с этими представлениями. Во-первых, они сохраняют все хорошие и традиционные свойства регистров сдвига с обратной связью по переносу (известный период, большая энтропия). Во-вторых, они обходят слабые стороны представлений Фибоначчи и Галуа. В-третьих, кольцевое представление обладает более быстрой диффузионной характеристикой и лучшими результатами реализации. Сведения о регистрах сдвига с обратной связью по переносу можно найти, например, в работе [4].

2. Структура функции. Внутренняя функция представляет собой перестановку, которую можно описать как последовательность операций над 2048-битовым состоянием S. Состояние S разбивается на 32 64-битовых слова $S_0, S_1, \ldots, S_{31}$. Слова записываются в матрицу 4×8 последовательно слева направо и сверху вниз. Четверки $S_i, S_{i+8}, S_{i+16}, S_{i+24}$, $i = 0, 1, \ldots, 7$, называются вертикальными плоскостями, а восьмерки $S_{8j}, S_{8j+1}, \ldots, S_{8j+7}$, $j = 0, 1, 2, 3$, — горизонтальными. Другими словами, состояние S можно рассматривать как трехмерный битовый массив: $S(x, y, z)$, $x = 0, 1, \ldots, 3$, $y = 0, 1, \ldots, 7$, $z = 0, 1, \ldots, 63$.

Действие внутренней функции состоит в 32-кратном повторении последовательности преобразований.

Преобразование 1:

$$f_1(S(x,y,z)) = S(x,y,z) + S(0,y-1,z) + S(1,y-1,z) + S(2,y-1,z) +$$
$$+ S(3,y-1,z) + S(0,y+1,z-1) + S(1,y+1,z-1) + S(2,y+1,z-1) + S(3,y+1,z-1)$$
$$\text{при} \quad x = 0,1,\ldots,3, \quad y = 1,\ldots,6, \quad z = 1,\ldots,63;$$
$$f_1(S(x,0,0)) = S(x,0,0) + S(0,7,0) + S(1,7,0) + S(2,7,0) + S(3,7,0) +$$
$$+ S(0,1,63) + S(1,1,63) + S(2,1,63) + S(3,1,63) \text{ при } x = 0,1,\ldots,3;$$
$$f_1(S(x,7,0)) = S(x,7,0) + S(0,6,0) + S(1,6,0) + S(2,6,0) + S(3,6,0) +$$
$$+ S(0,0,63) + S(1,0,63) + S(2,0,63) + S(3,0,63) \text{ при } x = 0,1,\ldots,3.$$

Преобразование 2:

$$f_2(S(x,y,z)) = S(x,y,z-(t+1)(t+2)/2),$$

где t такое, что $0 \leqslant t < 32$ и $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}^t \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ в $GF(4)^{2\times 2}$, или $t = -1$ при $x = y = 0$.

Преобразование 3:

$$f_3(S(x, y, z)) = S(x', y', z),$$

где x', y' такие, что $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$.

Преобразование 4: f_4 — оптимальный 8-битовый S-блок, применяемый к 8-битовым строкам $S(x, 0, z), S(x, 1, z), S(x, 2, z), S(x, 3, z), S(x, 4, z), S(x, 5, z), S(x, 6, z), S(x, 7, z)$. В данной статье он не определяется. Можно использовать уже существующие оптимальные S-блоки или сформировать с помощью известных методов генерации оптимальных S-блоков.

Преобразование 5: f_5 состоит в сложении слова S_{31} с 64-битовой константой C, которая вычисляется при помощи словарного регистра сдвига с обратной связью по переносу кольцевой конфигурации.

3. Анализ свойств преобразований. Преобразование f_1 является линейным. Его предназначение — обеспечение диффузии. Также оно инвариантно относительно сдвигов во всех направлениях. Его действие можно описать следующим образом: оно добавляет к каждому биту $S(x, y, z)$ побитовую сумму битов из двух столбцов: $S(x-1, *, z)$ и $S(x+1, *, z-1)$. Без преобразования f_1 внутренняя функция не будет обеспечивать диффузию какого-либо значения.

Преобразование f_2 состоит из перемещений внутри рядов, направленных на обеспечение межплоскостной дисперсии. Без него диффузия между плоскостями была бы очень медленной. Оно инвариантно относительно сдвигов в z-направлении. 32 сдвиговых констант определяются по формуле $i(i+1)/2$ по модулю длины ряда. Можно доказать, что для любого l последовательность $i(i+1)/2 \mod 2^l$ имеет период $2l+1$ и любая подпоследовательность с $n2^l \leqslant i < (n+1)2^l$ проходит через все значения Z_{2^l}. Из этого следует, что для рядов с длинами 64 и 32 все сдвиговые константы различны. Для рядов с длинами 16 и 9 сдвиговые константы встречаются дважды, с длиной 7 — один раз, с длинами 8, 4 и 2 — одинаково часто, за исключением сдвиговой константы 0, которая встречается на один раз чаще.

Преобразование f_3 является перемещением рядов. Его предназначение — обеспечение дисперсии, направленной на долгосрочную диффузию. Преобразование действует линейно по координатам (x, y): ряд в положении (x, y) переходит в положение $(x, y)M^T$, где $M = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix}$ — матрица размером 2×2 с элементами из $GF(4)$. Отсюда вытекает, что ряд в начале координат (0, 0) не меняет своего положения. Поскольку преобразование работает на плоскостях независимо, оно инвариантно относительно сдвигов в направлении z.

Преобразование f_4 есть единственное нелинейное отображение во внутренней функции. Без него раундовая функция была бы линейной. Его можно рассматривать как параллельное применение 256 8-битовых S-блоков.

S-блоки относятся к основным компонентам, определяющим нелинейность и уровень стойкости алгоритма. Для защиты алгоритма от различных типов атак S-блоки должны соответствовать ряду критериев. Из-за большого количества существующих критериев, их противоречивости или частичной взаимозависимости проблематично сформировать S-блок, обладающий всеми известными заданными свойствами. По-

этому на практике используются S-блоки, удовлетворяющие главным критериям, существенным для конкретного симметричного алгоритма. Такие S-блоки принято называть оптимальными. Критерии оптимального S-блока могут быть установлены для целого класса криптографических алгоритмов, а также заданы и для отдельно взятого криптопримитива. При выборе таблиц замен для новых шифров основными критериями служат нелинейность и дифференциальная равномерность. Дифференциальная равномерность является показателем стойкости против дифференциальной атаки. Например, для 8-битных подстановок оптимальны для дифференциальной равномерности значения не больше 8. Нелинейность — показатель стойкости против линейной атаки. Оптимальными для 8-битных подстановок являются значения не меньше 100. Алгебраическая степень и алгебраический иммунитет есть показатели стойкости против алгебраических атак. В случае 8-битных подстановок к оптимальным для алгебраической степени относятся значения не меньше 7, а максимальным для алгебраического иммунитета считается 3 при 441 уравнении. В случае подстановок 4 в 4 бита критерий алгебраического иммунитета не играет большой роли, так как они могут быть описаны системой уравнений второй степени. Но в то же время он не может равняться 1. Еще одним критерием служит отсутствие циклов длины 1, т. е. неподвижных (фиксированных) точек. Существует и множество других критериев. Современные критерии ориентированы на защиту от существующих видов криптоанализа: линейного, алгебраического и различных вариаций дифференциального. Еще один критерий связан с принадлежностью подстановок к разным классам эквивалентности векторных булевых функций. Он используется лишь в том случае, когда в алгоритме применяется более одного узла нелинейной замены. Многие исследования показывают, что идеальных S-блоков, вероятнее всего, нет. Поэтому было введено понятие оптимального S-блока, критерии которого определяются для конкретного криптографического алгоритма (или класса криптографических алгоритмов) и являются оптимальными с точки зрения защиты от существующих видов атак.

В настоящей статье S-блоки для преобразования f_4 не определяются. Можно использовать уже существующие оптимальные S-блоки или сформировать с помощью известных методов генерации оптимальных S-блоков. Сведения о методах генерации оптимальных S-блоков можно найти, например, в работах [5–14].

Преобразование f_5 состоит из сложения раундовых констант и направлено на нарушение симметрии. Без него раундовая функция была бы инвариантной относительно сдвигов в направлении z, и все раунды были бы равны, что делало бы внутреннюю функцию подверженной атакам, использующим симметрию, таким как, например, слайдовая атака. Биты раундовых констант различны от раунда к раунду и принимаются в качестве выходных данных словарного регистра сдвига с обратной связью по переносу кольцевой конфигурации. Константы добавляются только в одном ряде состояния. Из-за этого нарушение распространяется через f_1 и f_4 на все ряды в течение одного раунда.

4. Заключение. В настоящей статье предложен новый вариант внутренней функции, лежащей в основе перспективной современной схемы построения криптографических хеш-функций Sponge (криптографическая губка). Описываемый пример аналогичен перестановке Keccak, но имеет некоторые отличия. Внутренняя функция оперирует над 2048-битовым состоянием S, который можно рассматривать как трехмерный битовый массив размером $4 \times 8 \times 64$. Структуру внутренней функции составляют 5 преобразований f_1, f_2, f_3, f_4, f_5, аналогичных Keccak, но, во-первых, вместо

5-битового S-блока используется 8-битовый, во-вторых, для формирования раундовых констант вместо регистра сдвига с линейной обратной связью применяется словарный регистр сдвига с обратной связью по переносу кольцевой конфигурации. Проведен анализ свойств таких преобразований.

Литература

1. *Bertoni G., Daemen J., Peeters M., Assche G. V.* Sponge functions. Barcelona: Ecrypt Hash Workshop, 2007. 22 p. URL: http://keccak.team/files/SpongeFunctions.pdf (дата обращения: 15.11.2020).

2. *Bertoni G., Daemen J., Peeters M., Van Assche G.* Cryptographic sponge functions. Version 0.1. January 14, 2011. URL: http://keccak.team/files/CSF-0.1.pdf (дата обращения: 15.11.2020).

3. *Bertoni G., Daemen J., Peeters M., Van Assche G.* The Keccak reference. SHA-3 competition (round 3), 2011. URL: http://keccak.team/sponge_duplex.html (дата обращения: 15.11.2020).

4. *Arnault F., Berger T. P., Lauradoux C., Minier M., Pousse B.* A new approach for FCSRs // Cryptology ePrint Archive. Report 2009/167. 2009. URL: http://eprint.iacr.org/2009/167 (дата обращения: 15.11.2020).

5. *Nizam Chew L. C., Ismail E. S.* S-box construction based on linear fractional transformation and permutation function // Symmetry. 2020. Vol. 12. Art. N 826. https://doi.org/10.3390/sym12050826

6. *Zahid A. H., Arshad M. J.* An innovative design of substitution-boxes using cubic polynomial mapping // Symmetry. 2019. Vol. 11. Art. N 437. https://doi.org/10.3390/sym11030437

7. *Altaleb A., Saeed M. S., Hussain I., Aslam M.* An algorithm for the construction of substitution box for block ciphers based on projective general linear group // AIP Advances. 2017. Vol. 7. Art. N 035116. https://doi.org/10.1063/1.4978264

8. *Hussain S., Jamal S. S., Shah T., Hussain I.* A power associative loop structure for the construction of non-linear components of block cipher // IEEE Access. 2020. Vol. 8. P. 123492–123506.

9. *Gao W., Idrees B., Zafar S., Rashid T.* Construction of nonlinear component of block cipher by action of modular group $PSL(2, Z)$ on projective line $PL(GF(2^8))$ // IEEE Access. 2020. Vol. 8. P. 136736–136749.

10. *Казимиров А.В.* Методы и средства генерации нелинейных узлов замены для симметричных криптоалгоритмов: дисс. канд. техн. наук. Харьков: Харьк. нац. ун-т радиоэлектроники, 2013. 190 с.

11. *Rodinko M., Oliynykov R., Gorbenko Y.* Optimization of the high nonlinear S-boxes generation method. Bratislava: Tatra Mountains Mathematical Publ., Mathematical Institute, Slovak Academy of Sciences, 2017. Vol. 70. Iss. 1. P. 93–105.

12. *Ivanov G., Nikolov N., Nikova S.* Cryptographically strong S-boxes generated by modified immune algorithm // Cryptography and Information Security in the Balkans (BalkanCryptSec 2015). Eds by E. Pasalic, L. Knudsen. Cham: Springer, 2016. P. 31–42. (Lecture Notes in Computer Science. Vol. 9540.)

13. *Gorbenko I., Kuznetsov A., Gorbenko Y., Pushkar'ov A., Kotukh Y., Kuznetsova K.* Random S-boxes generation methods for symmetric cryptography // 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON). Lviv, Ukraine, 2019. P. 947–950.

14. *Easttom C.* A generalized methodology for designing non-linear elements in symmetric cryptographic primitives // 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). Las Vegas: NV, 2018. P. 444–449.

Статья поступила в редакцию 8 января 2021 г.
Статья принята к печати 4 июня 2021 г.

Контактная информация:

Оспанов Руслан Маратович — ст. науч. сотр.; ospanovrm@gmail.com

Сейткулов Ержан Нураханович — канд. физ.-мат. наук, доц.; yerzhan.seitkulov@gmail.com

Сисенов Нурбек Маханбетович — докторант, науч. сотр.; nurbek9291@mail.ru

Ергалиева Бану Бакытжановна — науч. сотр.; ergalieva_banu@mail.ru

An example of an internal function for the SPONGE scheme*

R. M. Ospanov, Ye. N. Seitkulov, N. M. Sissenov, B. B. Yergaliyeva

Gumilyov Eurasian National University, 2, ul. Satpayeva, Nur-Sultan, 010000, Kazakhstan

For citation: Ospanov R. M., Seitkulov Ye. N., Sissenov N. M., Yergaliyeva B. B. An example of an internal function for the SPONGE scheme. *Vestnik of Saint Petersburg University. Applied Mathematics. Computer Science. Control Processes*, 2021, vol. 17, iss. 3, pp. 287–293. https://doi.org/10.21638/11701/spbu10.2021.306 (In Russian)

The article discusses a new version of the internal function underlying the perspective modern scheme for constructing cryptographic hash functions Sponge (cryptographic sponge). The considered example of an internal function is similar to the Keccak permutation, but it has a number of main differences. The inner function operates on a 2048-bit state S, which can be viewed as a three-dimensional bit array of $4 \times 8 \times 64$ size. The structure of the internal function is made up of 5 transformations similar to Keccak. However, firstly, in this example, instead of a 5-bit S-box, an 8-bit one is used. In this regard, the parameters of the three-dimensional representation of the state have been changed. Secondly, instead of a linear feedback shift register, a dictionary shift register with ring carry feedback is used to generate round constants. The properties of these transformations are analyzed in the work.

Keywords: information security, cryptography, hash function, Sponge modification, symmetric encryption.

References

1. Bertoni G., Daemen J., Peeters M., Assche G. V. *Sponge functions*. Barcelona, Ecrypt Hash Workshop Press, 2007, 22 p. Available at: http://keccak.team/files/SpongeFunctions.pdf (accessed: November 15, 2020).

2. Bertoni G., Daemen J., Peeters M., Van Assche G. V. *Cryptographic sponge functions*. Version 0.1. January 14, 2011. Available at: http://keccak.team/files/CSF-0.1.pdf (accessed: November 15, 2020).

3. Bertoni G., Daemen J., Peeters M., Van Assche G. V. *The Keccak reference*. SHA-3 competition (round 3), 2011. Available at: http://keccak.team/sponge_duplex.html (accessed: November 15, 2020).

4. Arnault F., Berger T. P., Lauradoux C., Minier M., Pousse B. A new approach for FCSRs. *Cryptology ePrint Archive*. Report 2009/167, 2009. Available at: http://eprint.iacr.org/2009/167 (accessed: November 15, 2020).

5. Nizam Chew L. C., Ismail E. S. S-box construction based on linear fractional transformation and permutation function. *Symmetry*, 2020, vol. 12, Art. no. 826. https://doi.org/10.3390/sym12050826

6. Zahid A. H., Arshad M. J. An innovative design of substitution-boxes using cubic polynomial mapping. *Symmetry*, 2019, vol. 11, Art. no. 437. https://doi.org/10.3390/sym11030437

7. Altaleb A., Saeed M. S., Hussain I., Aslam M. An algorithm for the construction of substitution box for block ciphers based on projective general linear group. *AIP Advances*, 2017, vol. 7, Art. no. 035116. https://doi.org/10.1063/1.4978264

8. Hussain S., Jamal S. S., Shah T., Hussain I. A power associative loop structure for the construction of non-linear components of block cipher. *IEEE Access*, 2020, vol. 8, pp. 123492–123506.

9. Gao W., Idrees B., Zafar S., Rashid T. Construction of nonlinear component of block cipher by action of modular group $PSL(2, Z)$ on projective line $PL(GF(2^8))$. *IEEE Access*, 2020, vol. 8, pp. 136736–136749.

10. Kazymyrov O. *Metody i sredstva generatsii nelineinykh uzlov zameny dlia simmetrichnykh kriptoalgoritmov*. Dissertatsiia na soiskanie uchenoi stepeni kandidata tekhnicheskikh nauk [*Methods and tools to generate nonlinear substitution boxes for symmetric cryptographic algorithms*. Diss. PhD in Technics]. Kharkiv, Kharkiv National University of Radio Electronics, 2013, 190 p. (In Russian)

* This work was supported by the «Ministry of Digital Development, Innovations and Aerospace Industry of the Kazakhstan Republic» (project N AP06851124).

11. Rodinko M., Oliynykov R., Gorbenko Y. *Optimization of the high nonlinear S-boxes generation method.* Bratislava, Tatra Mountains Mathematical Publ., Mathematical Institute, Slovak Academy of Sciences, 2017, vol. 70, iss. 1, pp. 93–105.

12. Ivanov G., Nikolov N., Nikova S. Cryptographically strong S-boxes generated by modified immune algorithm. *Cryptography and Information Security in the Balkans (BalkanCryptSec 2015).* Eds by E. Pasalic, L. Knudsen. Cham, Springer Publ., 2016, pp. 31–42. (Lecture Notes in Computer Science, vol. 9540.)

13. Gorbenko I., Kuznetsov A., Gorbenko Y., Pushkar'ov A., Kotukh Y., Kuznetsova K. Random S-boxes generation methods for symmetric cryptography // *2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON).* Lviv, Ukraine, 2019, pp. 947–950.

14. Easttom C. A generalized methodology for designing non-linear elements in symmetric cryptographic primitives. *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC).* Las Vegas, NV Press, 2018, pp. 444–449.

Received: January 08, 2021.
Accepted: June 04, 2021.

A u t h o r s' i n f o r m a t i o n:

Ruslan M. Ospanov — Elder Researcher; ospanovrm@gmail.com

Yerzhan N. Seitkulov — PhD in Physics and Mathematics, Associate Professor; yerzhan.seitkulov@gmail.com

Nurbek M. Sissenov — Researcher; nurbek9291@mail.ru

Banu B. Yergalieva — Researcher; ergalieva_banu@mail.ru