МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 2 С. 7 –28

УДК 519.719.2

Bash-f: another LRX sponge function

S. Agievich, V. Marchuk, A. Maslau, V. Semenov

Belarusian State University, Belarus

Получено 16.III.2016

Abstract. We present the `Bash` family of hashing algorithms based on the sponge paradigm. A core element of this family is the `Bash-f` sponge function which refers to the LRX (Logical-Rotation-Xor) class of symmetric cryptographic schemes. We describe the components of `Bash-f`: a nonlinear mapping, linear diffusion mappings, a permutation of words of a hash state. For each component we establish reasonable quality criteria aiming to make the choice of components maximally objective and transparent.

Key words: hash algorithm, sponge construction, LRX, S-box, bitslice technique

Bash-f: вариант LRX хэш-функции типа «губка»

С. Агиевич, В. Марчук, А. Маслау, В. Семенов

Белорусский государственный университет, Белоруссия

Аннотация. Предлагается семейство функций хэширования `Bash`, основанных на конструкции «губка». Основным элементом этого семейства является функция `Bash-f`, которая относится к LRX (Logical-Rotation-Xor) классу симметричных криптографических алгоритмов. Описаны компоненты `Bash-f`: нелинейное преобразование, линейные рассеивающие преобразования, перестановка векторов состояния функции. Для каждой компоненты мы определяем критерии качества таким образом, чтобы обеспечить возможность максимально объективного и прозрачного выбора компонент.

Ключевые слова: хэш-функция, конструкция «губка», LRX, S-блок, техника битслайс

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 2, pp. 7–28 (Russian)

References

[1] “Bee2: A cryptographic library”, Avail. at https://github.org/agievich/bee2.

[2] Bertoni G., Daemen J., Peeters M., Van Assche G., “Cryptographic sponge functions. Version 0.1” (2011), Avail. at http://sponge.noekeon.org/CSF-0.1.pdf.

[3] Bertoni G., Daemen J., Peeters M., Van Assche G., “Sponge functions”. In: “*Ecrypt Hash Workshop*”, 2007.

[4] Brouwer A. E., Hobart S. A., “Parameters of directed strongly regular graphs”, Avail. at http://homepages.cwi.nl/ aeb/math/dsrg/dsrg.html.

[5] *Cryptography standards of Belarus* (in Russian), Avail. at http://apmi.bsu.by/resources /std.

[6] Harrison M. A., “On the classification of Boolean functions by the general linear and affine group”, *J. SIAM*, **12** (1964), 284–299.

[7] Jorgensen L. K., “Directed strongly regular graphs with $\mu = \lambda$”, *Discrete Math.*, **231** (2001), 289–293.

[8] Lidl R., Niederreiter H., *Finite Fields*, Cambridge: Cambridge Univ. Press, 1997, 755 pp.

[9] Lorens C. S., “Invertible Boolean Functions”, *IEEE Transactions on Electronic Computers*, **13**:5 (1964), 529–541.

[10] Bertoni G., Daemen J., Peeters M., Van Assche G., Van Keer R., “Keccak implementation overview”, Avail. at http://keccak.noekeon.org/Keccak-implementation-3.2.pdf.

[11] Bernstein D. J., Lange T. (editors), *eBACS: ECRYPT Benchmarking of Cryptographic Systems*, https://bench.cr.yp.to.