На втором шаге анализируем полученную конструкцию и показываем, что выходы обоих оракулов можно промоделировать без знания открытого текста. Итоговые оценки получаются из предположения, что множества, на которых вычисляются значения подстановок $\pi(x)$ и $\pi^{-1}(x)$, не пересекаются.

Полученная оценка близка к оптимальной для стандартного режима CBC: член вида $O((qm)^2/2^n)$ отражает тот факт, что для режима CBC всегда существует атака дней рождения, предполагающая возникновение коллизии для векторов инициализации IV.

ЛИТЕРАТУРА

1. *Katz J. and Lindell Y.* Introduction to Modern Cryptography, 2nd Ed. Chapman & Hall/CRC, 2014.
2. Межгосударственный стандарт ГОСТ 34.13-2018 Информационная технология (ИТ). Криптографическая защита информации. Режимы работы блочных шифров. М.: Стандартинформ, 2018.
3. *Ahmetzyanova L. R., Alekseev E. K., Oshkin I. B., et al.* On the properties of the CTR encryption mode of Magma and Kuznyechik block ciphers with re-keying method based on CryptoPro Key Meshing // Матем. вопр. криптогр. 2017. Т. 8. №2. С. 39–50.
4. *Rogaway P.* Evaluation of Some Block Cipher Modes of Operation. 2011. `https://web.cs.ucdavis.edu/~rogaway/papers/modes.pdf`
5. *Wooding M.* New Proofs for Old Modes. IACR Cryptology ePrint Archive. 2008.
6. *Bellare M., Desai A., Jokipii E., and Rogaway P.* A concrete security treatment of symmetric encryption // Proc. 38th Ann. Symp. Foundations of Computer Science, IEEE, 1997. P. 394–403.

УДК 519.714.5 DOI 10.17223/2226308X/13/21

ОБ ОДНОМ ПОДХОДЕ К ПОСТРОЕНИЮ КРАТНО ТРАНЗИТИВНОГО МНОЖЕСТВА БЛОЧНЫХ ПРЕОБРАЗОВАНИЙ

И. В. Чередник

Пусть Ω — произвольное конечное множество; $\mathcal{B}(\Omega)$ — семейство всех бинарных операций, определённых на Ω; $x_1, \ldots, x_n$ — переменные, принимающие значения из Ω; $*_1, \ldots, *_k$ — общие символы бинарных операций. Фиксированный набор $W = (w_1, \ldots, w_m)$ формул в алфавите $\{x_1, \ldots, x_n, *_1, \ldots, *_k\}$ при замене $*_1, \ldots, *_k$ на произвольные бинарные операции $F_1, \ldots, F_k \in \mathcal{B}(\Omega)$ соответственно реализует отображение $W^{F_1,\ldots,F_k}\colon \Omega^n \to \Omega^m$. Исследованы криптографические свойства (биективность и кратная транзитивность) семейств блочных преобразований $\{W^{F_1,\ldots,F_k} : F_1, \ldots, F_k \in \mathcal{K}\}$, $\mathcal{K} \subset \mathcal{B}(\Omega)$, которые могут быть использованы при построении хэш-функций и блочных шифров.

Ключевые слова: *блочные преобразования, кратная транзитивность множества блочных преобразований, функциональная бинарная сеть.*

В последнее время при разработке систем защиты информации активно исследуется возможность использования неассоциативных алгебраических структур, особое место в таких исследованиях занимают квазигруппы. Например, в ряде схем поточных шифров, хеш-функций и др. [1–3] используются семейства блочных преобразований, реализуемых наборами «цепных» формул вида

$$C_a^*(x_1, \ldots, x_n) = (a * x_1, (a * x_1) * x_2, \ldots, ((a * x_1) * \ldots) * x_n), \quad a \in \Omega,$$

где $*$ — квазигрупповая операция на некотором конечном множестве Ω. При этом в подавляющем большинстве схем подобного рода квазигрупповая операция $*$ выбирается из небольшого множества отобранных квазигрупп $\{*_1, \ldots, *_k\}$ и параметризация соответствующих блочных преобразований $C_a^*\colon \Omega^n \to \Omega^n$ достигается в основном за счёт выбора «начального» элемента $a \in \Omega$.

Одной из желаемых характеристик семейств блочных преобразований, используемых в узлах защиты информации, является кратная транзитивность данного семейства. Однако неизвестно, являются ли классы блочных преобразований типа

$$\left\{C_{a_1}^{*i_1} \cdot \ldots \cdot C_{a_r}^{*i_r} : \ a_1, \ldots, a_r \in \Omega, \ i_1, \ldots, i_r \in \{1, \ldots, k\}\right\}$$

хотя бы транзитивными, при этом отсутствуют практически эффективные методы, которые позволяли бы это выяснить.

В данной работе предлагается концепция построения классов блочных преобразований, при которой параметризация отображений достигается исключительно за счет широкого выбора бинарных операций. Пусть Ω — произвольное конечное множество; $\mathcal{B}(\Omega)$ — множество всех бинарных операций, определённых на Ω; $\{x_1, \ldots, x_n\}$ — множество переменных и $*_1, \ldots, *_k$ — символы бинарных операций. Произвольная формула $w(x_1, \ldots, x_n)$ в алфавите $\{x_1, \ldots, x_n, *_1, \ldots, *_k\}$ при сопоставлении символам $*_1, \ldots, *_k$ конкретных бинарных операций $F_1, \ldots, F_k \in \mathcal{B}(\Omega)$ соответственно реализует функцию $w^{F_1,\ldots,F_k}\colon \Omega^n \to \Omega$, а набор формул $W = (w_1, \ldots, w_m)$ — отображение $W^{F_1,\ldots,F_k}\colon \Omega^n \to \Omega^m$.

Предложенная концепция во многом происходит от практики, поскольку при проведении анализа узлов переработки информации часто возникает задача исследования семейств отображений вида

$$\{W^{F_1,\ldots,F_k} : F_1, \ldots, F_k \in \mathcal{K}\}, \quad \mathcal{K} \subset \mathcal{B}(\Omega). \tag{1}$$

Так, например, в некоторых случаях наличие запретов в совместных распределениях нескольких отображений из класса (1) позволяет идентифицировать начальные состояния и часть постоянных параметров изучаемых узлов.

Отметим также, что изложенная концепция в случае использования одной бинарной операции уже рассматривалась в работах [4–9]. Так, в работе [5] для некоторых семейств преобразований

$$\{W^F : F \in \mathcal{Q}(\Omega)\} \tag{2}$$

($\mathcal{Q}(\Omega)$ — множество всех бинарных квазигрупп, заданных на Ω) предложена модель наглядного описания в виде бинарной функциональной схемы-сети. Указанное представление позволило в работах [5, 7] строго описать и обосновать методы исследования кратной транзитивности классов преобразований вида (2). Кроме того, в [5, 7] изложены алгоритмы построения семейств вида (2) с требуемой кратной транзитивностью. Однако в большинстве узлов защиты информации вовсе не требуется использование квазигруппы, и достаточно бинарной операции, обратимой по одной, например правой, переменной. Поэтому в [8, 9] исследована возможность продолжения результатов работ [5, 7] на более широкий по сравнению с $\mathcal{Q}(\Omega)$ класс $\mathcal{B}^*(\Omega)$ всех бинарных операций, обратимых по правой переменной.

В данной работе получено следующее продолжение результатов [5, 7–9]:

1) предложенная в [5] модель наглядного представления семейств преобразований типа (2) в виде бинарной функциональной схемы-сети пригодна также

для представления произвольных семейств преобразований вида (1) и позволяет строго описать методы исследования кратной транзитивности произвольных семейств преобразований вида (1) для любого класса $\mathcal{K}$, удовлетворяющего условию $\mathcal{Q}(\Omega) \subset \mathcal{K} \subset \mathcal{B}^*(\Omega)$;

2) все основные результаты работ [5, 7–9] корректным образом распространяются на случай использования нескольких бинарных операций — такой более общий подход улучшает характеристики практического использования кратно транзитивных семейств преобразований, предложенных в [7, 9], а кроме того, позволяет «аппроксимировать» некоторые известные блочные шифры, в которых S-боксы зависят от ключа, (Blowfish, Twofish и др.) семействами блочных преобразований вида (1), и, как следствие, появляется возможность оценить кратную транзитивность указанных блочных шифров.

ЛИТЕРАТУРА

1. *Gligoroski D., Markovski S., Kocarev L., and Gusev M.* Edon80. `http://www.ecrypt.eu.org/stream/edon80p3.html` — eSTREAM, ECRYPT Stream Cipher Project.
2. *Gligoroski D., Markovski S., and Kocarev L.* Edon-R, An infinite family of cryptographic hash functions. `http://csrc.nist.gov/pki/HashWorkshop/2006/Papers/GLIGOROSKI_EdonR-ver06.pdf` — Second NIST Cryptographic Hash Workshop.
3. *Gligoroski D., Markovski S., and Knapskog S.* A public key block cipher based on multivariate quadratic quasigroups. `http://eprint.iacr.org/2008/320` — Cryptology ePrint Archive.
4. *Чередник И. В.* Об одном подходе к построению транзитивного множества блочных преобразований // Прикладная дискретная математика. Приложение. 2017. №10. С. 27–29.
5. *Чередник И. В.* Один подход к построению транзитивного множества блочных преобразований // Прикладная дискретная математика. 2017. №38. С. 5–34.
6. *Чередник И. В.* k-Транзитивность одного класса блочных преобразований // Прикладная дискретная математика. Приложение. 2018. №11. С. 21–23.
7. *Чередник И. В.* Один подход к построению кратно транзитивного множества блочных преобразований // Прикладная дискретная математика. 2018. №42. С. 18–47.
8. *Чередник И. В.* Об использовании бинарных операций при построении транзитивного множества блочных преобразований // Дискретная математика. 2019. №31. Т. 3 С. 93–113.
9. *Чередник И. В.* Об использовании бинарных операций при построении кратно транзитивного множества блочных преобразований // Дискретная математика. 2020. Т. 32. №2. С. 85–111.

УДК 519.719.1 DOI 10.17223/2226308X/13/22

УТОЧНЕНИЕ СТРАТЕГИИ МАЙНИНГА ДЛЯ НЕБОЛЬШОЙ ГРУППЫ УЧАСТНИКОВ

А. В. Черемушкин

Ittay Eyal и Emin Gün Sirer описали стратегию проведения т. н. корыстного майнинга, показывающую уязвимость протокола формирования цепочки блоков, реализованного в биткоине, к атаке со стороны группы участников майнинга, составляющей относительно небольшую часть от общего числа майнеров, и позволяющую ей получить вознаграждение, превышающее размер доли имеющихся у них вычислительных ресурсов. В настоящей работе предложена уточнённая вероятностно-автоматная марковская модель, основанная на предположении о независимости обеих групп участников.