МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 1 С. 107–142

УДК 519.719.2+519.712

Разбиения на биграммах и марковость алгоритмов блочного шифрования

Б. А. Погорелов [1], **М. А. Пудовкина** [2]

[1] *Академия криптографии Российской Федерации, Москва*

[2] *Московский государственный технический университет имени Н. Э. Баумана, Москва*

Получено 20.IV.2015

Аннотация. Изучается модель итерационных алгоритмов блочного шифрования с независимыми и равновероятно выбираемыми раундовыми ключами, алфавитом текстов X и группой $(X, \otimes)$ наложения ключа. Указаны условия, обеспечивающие сохранение марковости при укрупнении цепи Маркова с множеством состояний X^2, соответствующей биграммам промежуточных текстов. Описаны свойства рассматриваемых марковских алгоритмов блочного шифрования и преобразований укрупнения.

Ключевые слова: марковский алгоритм блочного шифрования, цепи Маркова, укрупнение состояний, метод усеченных разностей

Partitions on bigrams and Markov property of block ciphers

B. A. Pogorelov [1], **M. A. Pudovkina** [2]

[1] *Academy of Cryptograpfy of the Russian Federation, Moscow*

[2] *Bauman Moscow State Technical University, Moscow*

Abstract. A model of iterated block ciphers with alphabet X, independent uniform round keys and a key addition group $(X, \otimes)$ is considered. We find conditions ensuring the preservation of Markov property under lumping of Markov chain with state space X^2 corresponding to bigrams of intermediate ciphertexts. We describe properties of Markov ciphers considered and lumping transforms.

Key words: Markov block cipher, Markov chain, states lumping, truncated differential technique

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 107–142 (Russian)

Список литературы

[1] Minier M., Gilbert H., “Stochastic cryptanalysis of Crypton”. In: “*FSE 2000*”, Lect. Notes Comput. Sci., **1978**, 2000, 121–133.

[2] Lai X., Massey J. L., Murphy S., “Markov ciphers and differential cryptanalysis”. In: “*EuroCrypt 1991*”, Lect. Notes Comput. Sci., **547**, 1991, 17–38.

[3] Кемени Д., Снелл Д., *Конечные цепи Маркова*, М. : Наука, 1970, 272 с.

[4] Сачков В. Н., “Вероятностные преобразователи и правильные мультиграфы. I”, *Труды по дискретной математике*, **1** (1997), 227–250.

[5] Сачков В. Н., “Цепи Маркова итерационных систем преобразований”, *Труды по дискретной математике*, **6** (2002), 165–183.

[6] Сачков В. Н., “Вероятностные преобразователи и суммы элементарных матриц. II”, *Труды по дискретной математике*, **8** (2005), 240–252.

[7] Максимов Ю. И., “Некоторые результаты для задачи укрупнения состояний цепей Маркова”, *Труды по дискретной математике*, **8** (2005), 148–154.

[8] Vaudenay S., “On the Lai – Massey scheme”. In: “*ASIACRYPT’99*”, Lect. Notes Comput. Sci., **1716**, 1999, 8–19.

[9] Knudsen L. R., “Truncated and higher order differentials”. In: “*FSE’95*”, Lect. Notes Comput. Sci., **1008**, 1995, 196–211.

[10] Matsui M., Tokita T., “Cryptanalysis of a reduced version of the block cipher E2”. In: “*FSE’99*”, Lect. Notes Comput. Sci., 1999, 70–79.

[11] Moriai S., Sugita M., Aoki K., Kanda M., “Security of E2 against truncated differential cryptanalysis”. In: “*SAC’99*”, Lect. Notes Comput. Sci., **1758**, 2000, 106–117.

[12] Reichardt B., Wagner D., “Markov truncated differential cryptanalysis of Skipjack”. In: “*SAC 2002*”, Lect. Notes Comput. Sci., **2595**, 2002, 110—128.

[13] Blondeau C., “Improbable differential from impossible differential: on the validity of the model”. In: “*INDOCRYPT 2013*”, Lect. Notes Comput. Sci., **8250**, 2013, 149–160.

[14] Massey J.L., “SAFER K-64: One year later”. In: “*FSE’94*”, Lect. Notes Comput. Sci., **1008**, 1994, 212–232.

[15] Lai X., *On the design and security of block ciphers*, Zurich, Swiss Federal Inst. Technology, PhD, 1992.

[16] Агиевич С. В., Афоненко А. А., “Экспоненциальные S-блоки”, В сб.: *Математика и безопасность информационных технологий*. МАБИТ 2003, М. : МЦНМО, 2003, 127–130.

[17] Шемякина О. В., “Об оценке характеристик разбиений различных алгебраических структур”, В сб.: Информ. безопасность регионов России ИБРР-2011. Матер. VII СПб. межрегион. конф., СПб. : СПОИСУ, 2011, 137.

[18] Nyberg K., Knudsen L. R., “Provable security against differential cryptanalysis”. In: “*Crypto 1992*”, Lect. Notes Comput. Sci., **740**, 1993, 566–574.