5. *Агибалов Г. П.* Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1. С. 34–42.
6. *Selcuk A. A.* On probability of success in linear and differential cryptanalysis // J. Cryptology. 2007. No. 21. P. 131–147.
7. *Пестунов А. И.* О связях между основными понятиями разностного анализа итеративных блочных шифров // Прикладная дискретная математика. Приложение. 2013. № 6. С. 44–48.
8. *Biryukov A. and Kushilevitz E.* Improved cryptanalysis of RC5 // LNCS. 1998. V. 1403. P. 85–99.
9. *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра MARS // Прикладная дискретная математика. 2009. № 4. С. 56–63.
10. *Пестунов А. И.* Дифференциальный криптоанализ блочного шифра CAST-256 // Безопасность информационных технологий. 2009. № 4. С. 57–62.
11. *Пестунов А. И.* О вероятности протяжки однобитовой разности через сложение и вычитание по модулю // Прикладная дискретная математика. 2012. № 4. С. 53–60.
12. *Пестунов А. И.* О влиянии веса Хэмминга разности двух величин на вероятность её сохранения после сложения и вычитания // Дискретный анализ и исследование операций. 2013. Т. 20. № 5. С. 58–65.

УДК 519.7

ОБ ОБОБЩЕНИЯХ МАРКОВСКОГО ПОДХОДА ПРИ ИЗУЧЕНИИ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

Б. А. Погорелов, М. А. Пудовкина

Рассматриваются свойства алгоритмов блочного шифрования Маркова при укрупнении состояний цепи Маркова, основанных на разбиениях множества открытых текстов. Показано, что такие укрупнения состояний цепи Маркова, порождённые последовательностью промежуточных шифртекстов i-го раунда, $i = 1, 2, \ldots$, алгоритма блочного шифрования, также являются цепью Маркова.

Ключевые слова: *алгоритм шифрования Маркова, цепь Маркова, XSL-алгоритмы шифрования, алгоритмы шифрования Фейстеля.*

В работе [1] введён термин «стохастический метод криптоанализа» как обобщение большого класса методов, основанных на построении некоторых l-раундовых характеристик. Такими методами являются линейный [2], разностный [3] и их обобщения. В стохастическом методе раундовой функции i-го раунда ставится в соответствие матрица $\mathbf{p}^{(i)}$ переходов блоков $(i-1)$-го раунда в блоки i-го раунда, $i = 1, \ldots, l$. Матрица вероятностей переходов блоков разбиения открытого текста $\mathbf{X}^{(0)}$ в блоки разбиения $\mathbf{X}^{(l)}$ шифртекста l-го раунда предполагается равной $\mathbf{p}^{[l]} = \prod_{i=1}^{l} \mathbf{p}^{(i)}$. Для данного предположения требуется, чтобы последовательность, порождённая промежуточными текстами, являлась цепью Маркова. При этом для применения атак на основе стохастического метода существенным является предположение о независимости раундовых ключей, которое используется в линейном методе и различных обобщениях разностного метода.

В данной работе рассматриваются свойства алгоритмов блочного шифрования Маркова при укрупнении состояний цепи Маркова, основанных на таких разбиениях $U = (U_1, \ldots, U_d)$ множества $X^{\times}$ (называемых далее $U^{(\mu)}$-разбиениями), что раз-

биение U порождает метрику на X, где $X^\times = X\backslash\{e\}$, e — единичный элемент абелевой группы $(X, \otimes)$ с бинарной операцией $\otimes$. Близкими к таким разбиениям являются W-разбиения, где под W-разбиением понимается разбиение множества X на блоки одинаковой мощности. В частности, если W_0 — произвольная подгруппа $(X, \otimes)$, то рассматриваемым W-разбиением является множество смежных классов группы $(X, \otimes)$ по подгруппе W_0. Заметим, что при рассмотрении разбиения $\{W_0\backslash\{e\}, \ldots, W_{r-1}\}$ естественным образом получается $U^{(\mu)}$-разбиение. Кроме того, W-разбиения позволяют для XSL-алгоритмов блочного шифрования учитывать не только строение слоя наложения ключа, но и строение линейного слоя. Например, это возможно, если W_0 — инвариантное подпространство линейного преобразования. Блоки $U^{(\mu)}$-разбиения интерпретируются как множества разностей пар открытого текста (шифртекста). Заметим, что разбиение $X^\times$ с блоками единичной длины применяется в разностном методе, а усечённые разности естественным образом задают W-разбиение.

Показано, что такие укрупнения состояний цепи Маркова, порождённые последовательностями промежуточных шифртекстов i-го раунда, $i = 1, 2, \ldots$, алгоритмов блочного шифрования, являются цепью Маркова. Для них выполнен перенос ряда результатов работы [4]. В частности, приведены условия, при которых алгоритмы блочного шифрования на основе схем XSL, Фейстеля и Лея — Месси [5] являются марковскими относительно рассматриваемых разбиений.

ЛИТЕРАТУРА

1. *Minier M. and Gilbert H.* Stochastic cryptanalysis of Crypton // FSE'00. LNCS. 2000. V. 1978. P. 121–133.
2. *Matsui M.* Linear cryptanalysis method for DES cipher // Eurocrypt. LNCS. 1993. V. 765. P. 386–397.
3. *Biham E. and Shamir A.* Differential Cryptanalysis of the Data Encryption Standard. Springer Verlag, 1993.
4. *Lai X., Massey J. L., and Murphy S.* Markov ciphers and differential cryptanalysis // Eurocrypt. LNCS. 1991. V. 547. P. 17–38.
5. *Vaudenay S.* On the Lai — Massey scheme // Asiacrypt. LNCS. 1999. V. 1716. P. 8–19.

УДК 519.7

О ВЕРОЯТНОСТЯХ r-РАУНДОВЫХ ПАР РАЗНОСТЕЙ XSL-АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ МАРКОВА С ПРИВОДИМЫМ ЛИНЕЙНЫМ ПРЕОБРАЗОВАНИЕМ

М. А. Пудовкина

Раундовая функция XSL-алгоритма блочного шифрования является композицией трёх преобразований: преобразования сдвига (сложение с ключом), нелинейного преобразования (s-бокса) и линейного преобразования. Для XSL-алгоритма блочного шифрования Маркова с приводимым линейным преобразованием вместо «классической» r-раундовой разностной характеристики в разностном методе рассматривается r-раундовая характеристика, заданная последовательностью смежных классов инвариантного подпространства линейного преобразования.

Ключевые слова: *алгоритм шифрования Маркова, инвариантное множество, приводимое линейное преобразование, разностная характеристика.*