работе рассматривается обобщение на случай произвольных функций k-значной логики с учётом асимптотических условий 1 и 2, при этом уравновешенности функций не требуется.

Обозначим $a_{\min} = \min\{a_0(f_1), \ldots, a_0(f_T)\}$, $a_{\max} = \max\{a_0(f_1), \ldots, a_0(f_T)\}$.

Теорема 1. Пусть $n, T \to \infty$, $|S| \to \Sigma \in \mathbb{N}$, $T/a_{\min} \to 0$. Тогда:

1) если параметр d меняется так, что $d\sum\limits_{t=1}^{T} \dfrac{N^n - a_0(f_t)}{a_0(f_t)N^n} \to \infty$, то

$$\mathbf{P}\{\tilde{S} \cap S = \varnothing\} \to 1;$$

2) если параметр d меняется так, что $d\sum\limits_{t=1}^{T} \dfrac{N^n - a_0(f_t)}{a_0(f_t)N^n} \to \varkappa \in (0, \infty)$ и $\dfrac{Td}{a_{\min}} < c$, $c = \mathrm{const} > 0$, то распределение случайной величины $|\tilde{S} \cap S|$ сходится к $\mathrm{Bi}(\Sigma, e^{-\varkappa})$ — биномиальному распределению с параметрами Σ и $e^{-\varkappa}$;

3) если параметр d меняется так, что $d\sum\limits_{t=1}^{T} \dfrac{N^n - a_0(f_t)}{a_0(f_t)N^n} \to 0$ и $a_{\max} < \dfrac{N^n}{2}$, то

$$\mathbf{P}\{S \subseteq \tilde{S}\} \to 1.$$

ЛИТЕРАТУРА

1. *Михайлов В. Г.* Оценка точности пуассоновской аппроксимации для числа пустых ячеек в равновероятной схеме размещения частиц комплектами и её применения // Труды Матем. ин-та им. В. А. Стеклова РАН. 2013. Т. 282. С. 165–180.

УДК 519.7

ВЛИЯНИЕ ВЕСА ХЭММИНГА РАЗНОСТИ НА ВЕРОЯТНОСТЬ ЕЁ СОХРАНЕНИЯ ПОСЛЕ АРИФМЕТИЧЕСКИХ ОПЕРАЦИЙ[1]

А. И. Пестунов

Теоретически исследована зависимость между вероятностью сохранения разности двух величин после их сложения (вычитания) по модулю с третьей равномерно распределённой величиной и весом Хэмминга этой разности. Под разностью понимается общепринятая в криптоанализе операция XOR. Доказано, что если старший бит разности равен 0, то вероятность её сохранения равна 2^{-h}, где h — вес Хэмминга разности, и равна $2^{-(h-1)}$, если старший бит разности равен 1.

Ключевые слова: *дифференциальный криптоанализ, разностный анализ, блочный шифр, вес Хэмминга.*

Дифференциальный криптоанализ [1] вместе со своими модификациями является распространённым подходом к анализу стойкости итеративных блочных шифров, однако далеко не всегда авторы дифференциальных атак обосновывают их строго математически. Тем не менее некоторые шаги в этом направлении предпринимаются. Так, в работе [2] предложена модель марковского шифра, в рамках которой вычисляются вероятности характеристик; там же сформулирована гипотеза стохастической эквивалентности, негласно подразумеваемая в более ранних работах. В [3] показана возможность создания шифра, доказуемо стойкого к дифференциальному криптоанализу, а в [4] разработана модель, позволяющая создать такой шифр. Работа [5] посвящена изложению дифференциального криптоанализа в общем виде применительно

[1]Работа поддержана грантом РФФИ, проект № 14-01-31484 (мол_а).

к произвольным итеративным блочным шифрам с аддитивным раундовым ключом. Автор [6] аналитически вычисляет вероятность успеха дифференциальной атаки в зависимости от параметров шифра. В [7] предложена формализация основных понятий дифференциального криптоанализа и проведена их систематизация.

Другой важной проблемой является изучение того, как изменяется разность блоков или подблоков после операций, используемых в блочных шифрах. При этом оценивается вероятность того, что пара величин с определённой разностью преобразуется заданной операцией в пару величин с такой же или другой, но определённой разностью. Для некоторых операций, например циклического сдвига или XOR, данная проблема решается тривиально, но для таких часто используемых операций, как сложение, вычитание и умножение по модулю изучение изменения разности нетривиально.

В работе, посвящённой дифференциальному криптоанализу шифра RC5 [8], утверждается, что однобитовая разность остаётся неизменной после операции сложения с вероятностью $1/2$ (или с вероятностью 1, если этот единственный бит — старший). Данное утверждение теоретически не доказывается, но проводятся эксперименты, подтверждающие достоверность разработанной атаки. В работах по дифференциальному криптоанализу шифров MARS [9] и CAST-256 [10] данный факт используется со ссылкой на [8] и последующими экспериментами, подтверждающими достоверность разработанных атак. В работе [11] этот факт доказан теоретически.

В [10] используется экспериментально найденная зависимость между весом Хэмминга разности и вероятностью её сохранения после сложения по модулю. В настоящей работе существование этой зависимости доказано теоретически и показано её существование для операции вычитания.

Используем обозначения: s — длина двоичного вектора (в битах); $X \sim \mathcal{U}\{0,1\}^s$ — X имеет равномерное распределение на $\{0,1\}^s$; $\boxplus, \boxminus$ — соответственно сложение и вычитание по модулю 2^s; δ_{s-1} — старший бит вектора Δ; $H(\Delta)$ — вес Хэмминга вектора Δ.

Основным результатом работы является следующая

Теорема 1. Пусть X, $Z \sim \mathcal{U}\{0,1\}^s$ и $Y = X \oplus \Delta$, где $H(\Delta) = h$, $0 \leqslant h \leqslant s-1$. Тогда

а) $\mathbf{P}\big((X \boxplus Z) \oplus (Y \boxplus Z) = \Delta\big) = 2^{-h}$, если $\delta_{s-1} = 0$;

б) $\mathbf{P}\big((X \boxplus Z) \oplus (Y \boxplus Z) = \Delta\big) = 2^{-(h-1)}$, если $\delta_{s-1} = 1$.

Следствие 1. Пусть X, $Z \sim \mathcal{U}\{0,1\}^s$ и $Y = X \oplus \Delta$, где $H(\Delta) = h$, $0 \leqslant h \leqslant s-1$. Тогда

а) $\mathbf{P}\big((X \boxminus Z) \oplus (Y \boxminus Z) = \Delta\big) = 2^{-h}$, если $\delta_{s-1} = 0$;

б) $\mathbf{P}\big((X \boxminus Z) \oplus (Y \boxminus Z) = \Delta\big) = 2^{-(h-1)}$, если $\delta_{s-1} = 1$.

Доказательства теоремы и следствия можно найти в [12].

ЛИТЕРАТУРА

1. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
2. *Lai X. and Massey J.* Markov ciphers and differential cryptanalysis // LNCS. 1991. V. 547. P. 17–38.
3. *Nyberg K. and Knudsen L.* Provable security against a differential attack // J. Cryptology. 1995. No. 8. P. 27–37.
4. *Vaudenay S.* Decorrelation: a theory for block cipher security // J. Cryptology. 2003. No. 16. P. 249–286.

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-