На практике число раундов алгоритма блочного шифрования выбирается превышающим экспонент примерно в 2 раза, чтобы любой промежуточный блок данных зависел от всех битов либо входного, либо выходного блока. Следовательно, достаточно реализовать 14 раундов шифрования для обеспечения требуемого перемешивания данных.

ЛИТЕРАТУРА

1. *Коренева А. М., Фомичев В. М.* Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика. 2012. №3 (в печати).

УДК 519.7, 004.056.2, 004.056.53

## РАЗНОСТНЫЕ УРАВНЕНИЯ ДЛЯ АЛГОРИТМОВ ХЭШИРОВАНИЯ СЕМЕЙСТВА MDx

С. Д. Лошкарёв

В работах [1, 2], описывающих хэш-функции семейства MDx, практически отсутствует обоснование выбора элементов алгоритма. Основная цель данной работы — исследовать влияние примитивных булевых функций и значений циклических сдвигов на стойкость хэш-функции MD5 к методам дифференциального криптоанализа в рамках модели, построенной в работе [3]. Данная модель позволяет количественно оценить устойчивость хэш-функции к дифференциальному криптоанализу. В рамках этой модели каждой хэш-функции ставится в соответствие разностное уравнение. Для шага преобразования хэш-функции MD5 это разностное уравнение имеет вид ($X_i$ — переменные, $A_i$ — параметры, $s$ — величина циклического сдвига на данном шаге)

$$(f(X_1{+}A_1, X_2{+}A_2, X_3{+}A_3){+}X_4{+}A_4) \lll s = (A_0 << s){+}(f(X_1, X_2, X_3){+}X_4) \lll s. \quad (1)$$

Далее в рассматриваемой модели поочередно фиксируются нулями все возможные сочетания параметров $A_i$ и для каждого зафиксированного набора строится величина $EP(f; \_, \_, \_, \_; s)$ (на месте $i$-го символа _ ставится 0, если параметр $A_i$ зафиксирован нулем, и $*$ — в противном случае) — среднее значение вероятности угадать решение данного уравнения, выбирая вектор $X = \{X_1, X_2, X_3, X_4\}$ случайно и равновероятно, при этом незафиксированные параметры $A_i$ принимают все возможные значения и по ним осуществляется усреднение. В соответствии с моделью для данного уравнения строится характеристический вектор $\chi_{32}(f, s)$, состоящий из 32 компонент, представляющих собой величины $EP(f; \_, \_, \_, \_; s)$ для всех вариантов фиксации параметров $A_i$.

В рамках модели [3], используя похожую аргументацию, можно показать, что хэш-функция MD5 с булевой функцией $f_2$ на фиксированном шаге при фиксированном значении циклического сдвига $s$ более устойчива к дифференциальному криптоанализу, чем MD5 с булевой функцией $f_1$ на том же шаге с тем же значением циклического сдвига, если $\chi_{32}(f_2, s) \prec \chi_{32}(f_1, s)$. Это сравнение формирует бинарное отношение на множестве булевых функций при фиксированном значении циклического сдвига $s$ и бинарное отношение на множестве циклических сдвигов при фиксированной булевой функции $f$.

Для анализа уравнения (1) требуется расмотреть уравнение

$$f(X_1{+}A_1{+}\alpha_1, X_2{+}A_2{+}\alpha_2, X_3{+}A_3{+}\alpha_3){+}A_4{+}X_4{+}\alpha_4 = f(X_1, X_2, X_3){+}X_4{+}A_0{+}\alpha_0, \quad (2)$$

в котором сравнение происходит по модулю $2^{32}$ и $\alpha_0$, $\alpha_1$, $\alpha_2$, $\alpha_3$, $\alpha_5 < 2$, $\alpha_4 < 3$. Для данного уравнения введём обозначения для следующих переносов из младших $n$ бит:

— $\gamma_i$ — в сумме $X_i + A_i + \alpha_i$, $i = 1, 2, 3$ ($\gamma_i < 2$);
— $\gamma_4$ — в сумме $f(X_1 + A_1 + \alpha_1, X_2 + A_2 + \alpha_2, X_3 + A_3 + \alpha_3) + X_4 + A_4 + \alpha_4$ ($\gamma_4 \leqslant 2$);
— $\gamma_0$ — в сумме $A_0 + f(X_1, X_2, X_3) + X_4 + \alpha_0$ ($\gamma_0 \leqslant 2$);
— $\gamma_5$ — в сумме $f(X_1, X_2, X_3) + X_4 + \alpha_5$ ($\gamma_5 < 2$).

Введём матрицы $M(f; A_0, A_1, A_2, A_3, A_4; n)$ ($n = 2, 3$), в которых индекс по строке в троичной системе счисления равен $\alpha_5||\ldots||\alpha_0$, индекс по столбцу в троичной системе счисления равен $\beta_5||\ldots||\beta_0$, а элементами матрицы являются вероятности угадать решение уравнения (2), такое, что приведенные выше переносы равны значениям $\beta_5, \ldots, \beta_0$.

Далее используются следующие операции над матрицами:
— $Q(M) : \mathbb{R}^{3^6 \times 3^6} \to \mathbb{R}^{3 \times 3^5}$, исключает все строки, кроме первых трёх, и складывает столбцы, номера которых не равны только в младшем троичном разряде;
— $R(M) : \mathbb{R}^{3^6 \times 3^6} \to \mathbb{R}^{3^5 \times 3}$, записывает в результирующую матрицу суммы столбцов с совпадающими разностями $\gamma_0 - \gamma_5$ (при $\gamma_0 - \gamma_5 \geqslant 0$) в столбец с номером, равным этой разности; удаляет строки, для номера которых $\alpha_0 \neq \alpha_5$ (теперь из-за уменьшения размера матрицы номер может быть представлен в виде строки $(\alpha_4||\ldots||\alpha_0)$); переставляет строки так, чтобы строка $(\alpha_4||\ldots||\alpha_0)$ заняла место строки $(\alpha_3||\ldots||\alpha_0||\alpha_4)$.
— $Tr(M)$ — след матрицы (сумма диагональных элементов).

**Теорема 1.** При нечётном значении циклического сдвига $s$ среднее $EP(f; \ldots; s)$ можно вычислить по формуле (под $B$ понимается множество $\{0,1\}$)

$$EP(f;\ldots;s) = \frac{1}{2^{kT}} Tr\left(Q\left(\left(\sum_{\substack{a_{j_i}\in B^3,\\ i=\overline{1,k}}} M(f;\ldots a_{j_i}\ldots;3)\cdot \sum_{\substack{a_{j_i}\in B^2,\\ i=\overline{1,k}}} M(f;\ldots a_{j_i}\ldots;2)\right)^{\frac{T-s-1}{2}-1}\right)\times\right.$$
$$\left.\times R\left(\left(\sum_{\substack{a_{j_i}\in B^3,\\ i=\overline{1,k}}} M(f;\ldots a_{j_i}\ldots;3)\cdot \sum_{\substack{a_{j_i}\in B^2,\\ i=\overline{1,k}}} M(f;\ldots a_{j_i}\ldots;2)\right)^{\frac{s-3}{2}}\right)\right).$$

При чётном значении циклического сдвига $s$ среднее $EP(\ldots)$ вычисляется по формуле

$$EP(f;\ldots;s) = \frac{1}{2^{kT}} Tr\left(Q\left(\left(\sum_{\substack{a_{j_i}\in B^2,\\ i=\overline{1,k}}} M(f;\ldots a_{j_i}\ldots;2)\right)^{(T-s)/2}\right)\times\right.$$
$$\left.\times\, R\left(\left(\sum_{\substack{a_{j_i}\in B^2,\\ i=\overline{1,k}}} M(f;\ldots a_{j_i}\ldots;2)\right)^{s/2}\right)\right).$$

Через $k$ обозначено количество незафиксированных компонент в описании среднего.

**Следствие 1.** Сложность построения характеристического вектора для булевой функции $f$ и фиксированного значения $s$ по формулам из теоремы 1 меньше, чем $2^{34}$ (при этом сложность построения того же характеристического вектора методом полного перебора больше чем $2^{288}$).

**Теорема 2.** Построенное бинарное отношение на множестве булевых функций при каждом зафиксированном значении циклического сдвига $s$ совпадает с отношением порядка, построенным в работе [3].

В [3] показано, что наименьшим элементом для этого отношения является функция XOR. Поэтому имеет место

**Следствие 2.** Использование булевой функции XOR в хэш-функции MD5 является оптимальным с точки зрения устойчивости MD5 к дифференциальному криптоанализу.

**Теорема 3.** В построенном бинарном отношении на множестве значений циклических сдвигов для каждой булевой функции все значения циклических сдвигов эквивалентны.

ЛИТЕРАТУРА

1. *Rivest R.* The MD4 message digest algorithm // LNCS. 1991. V. 537. P. 303–311.
2. *Rivest R.* The MD5 message digest algorithm // RFC 1321, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992.
3. *Нгуен Т. Х., Карпунин Г. А.* Оптимальность выбора функции xor в одной модели дифференциального криптоанализа хэш-функций семейства MDx // Материалы IV Междунар. научн. конф. по проблемам безопасности и противодействия терроризму и VII Общерос. научн. конф. «Математика и безопасность информационных технологий» (МАБиТ–2008), Москва, МГУ, 30 октября – 1 ноября 2008 г. М.: МЦНМО, 2009. С. 65–70.

УДК 519.151,519.725, 519.165

## ПРОБЛЕМЫ ПОЧТИ ПОРОГОВЫХ СХЕМ РАЗДЕЛЕНИЯ СЕКРЕТА

Н. В. Медведев, С. С. Титов

В настоящее время вопросы, связанные с криптографическими методами защиты информации и математическими задачами криптологии, являются чрезвычайно важными [1]. Такими, например, являются задачи делегирования прав, разграничения доступа к информации и разделения секрета. Одними из основных криптографических примитивов в теории и практике защиты информации являются схемы разделения секрета (СРС).

Основная идея СРС состоит в предоставлении участникам долей секрета таким образом, чтобы только заранее заданные разрешённые коалиции участников могли однозначно восстановить секрет, а неразрешённые не получали никакой дополнительной к имеющейся априорной информации о возможном значении секрета [2].

В работе [3] описаны идеальные почти пороговые СРС, основанные на эллиптических кривых и позволяющие реализовать более сложную, чем у пороговых СРС, структуру доступа [4], при которой не все $n$-элементные множества участников могут однозначно восстановить секрет. Эллиптическая кривая и точки на ней используются для параметризации участников. В работе [5] доказано, что можно реализовать такую СРС с бесконечным количеством участников, где всюду плотность расположения рациональных точек на эллиптической кривой выступает аналогом совершенности.

Разрешённые коалиции идеальной совершенной схемы разделения секрета определяются циклами некоторого связного матроида, изучение которого и даёт структуру доступа [2], в данном случае матроиды будут почти пороговыми [3].