УДК 519.6

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА БЛОЧНЫХ ШИФРОВ, ПОСТРОЕННЫХ НА ОСНОВЕ РЕГИСТРОВ СДВИГА

А. М. Коренева, В. М. Фомичев

В некоторых приложениях целесообразно использовать блочные шифры с большим размером блоков данных. В связи с этим актуальным является исследование криптографических свойств симметричных блочных шифров на основе преобразований регистра сдвига произвольной длины над множеством r-мерных векторов, являющихся обобщением шифров Фейстеля [1].

Доклад посвящён рассмотрению инволютивного алгоритма блочного шифрования на основе регистра сдвига длины 4 над множеством двоичных 16-мерных векторов. Результаты работы [1] применяются для оценки перемешивающих свойств раундовой подстановки.

Пример инволютивного алгоритма блочного шифрования

Размер блока данных x равен 64 битам, длина раундового ключа z — 32 бита, число циклов шифрования h — 16. Блок x разбивается на четыре подблока x_1, x_2, x_3, x_4 размера 16 битов. Раундовый ключ z разбивается на два подключа z^1 и z^2 по 16 битов. Функция усложнения $\psi(x_2, x_3, x_4, z)$ (основной элемент цикловой подстановки) состоит из трёх конструктивных слоев:

1. Подмешивание ключа реализуется с помощью функции

$$M(x_2, x_3, x_4, z) = \{x_2 \oplus z^1, x_3 \oplus z^2, x_4 \oplus z^1\}.$$

2. Применение s-боксов — нелинейного преобразования S.

Пусть $M(x_2, x_3, x_4, z) = (y_1, y_2, y_3)$ и имеются совершенные преобразования s_{11}, s_{12}, s_{13}, s_{14}, s_{21}, s_{22}, s_{23}, s_{24} множества V_4, то есть каждый бит выхода любой из этих функций существенно зависит от всех четырёх битов входа.

При $y_1, y_2, y_3 \in V_{16}$ применим к (y_1, y_2, y_3) преобразование $S(y_1, y_2, y_3) = (S_1(y_1), S_2(y_2), S_1(y_3))$, где S_1 и S_2 суть преобразования множества V_{16} и для $b = (b_1, \ldots, b_{16}) \in V_{16}$ значение $S_i(b)$ определено следующей формулой, $i = 1, 2$:

$$S_i(b) = (s_{i1}(b_1, \ldots, b_4), s_{i2}(b_5, \ldots, b_8), s_{i3}(b_9, \ldots, b_{12}), s_{i4}(b_{13}, \ldots, b_{16})).$$

При выполнении преобразований S_1 и S_2 4-битовые выходы s-боксов соединяются в 16-битовые векторы $S_1(y_1), S_2(y_2), S_1(y_3)$, которые затем суммируются:

$$(a_1, a_2, \ldots, a_{16}) = S_1(y_1) \oplus S_2(y_2) \oplus S_1(y_3).$$

3. Перемешивание координат, T^{11} — циклический левый сдвиг на 11 битов:

$$T^{11}(a_1, a_2, \ldots, a_{16}) = (a_{12}, \ldots, a_{16}, a_1, \ldots, a_{11}).$$

Следовательно, функция усложнения $\psi(x_2, x_3, x_4, z)$ при ключе z имеет вид

$$\psi(x_2, x_3, x_4, z) = T^{11}\left(\sum(S(M(x_2, x_3, x_4, z)))\right).$$

При данной функции ψ алгоритм шифрования инволютивен [1, теорема 1] и каждый бит выхода функции усложнения ψ зависит существенно от 12 битов множества векторов $\{x_2, x_3, x_4\}$. Схема реализации раундовой подстановки шифра дана на рис. 1.

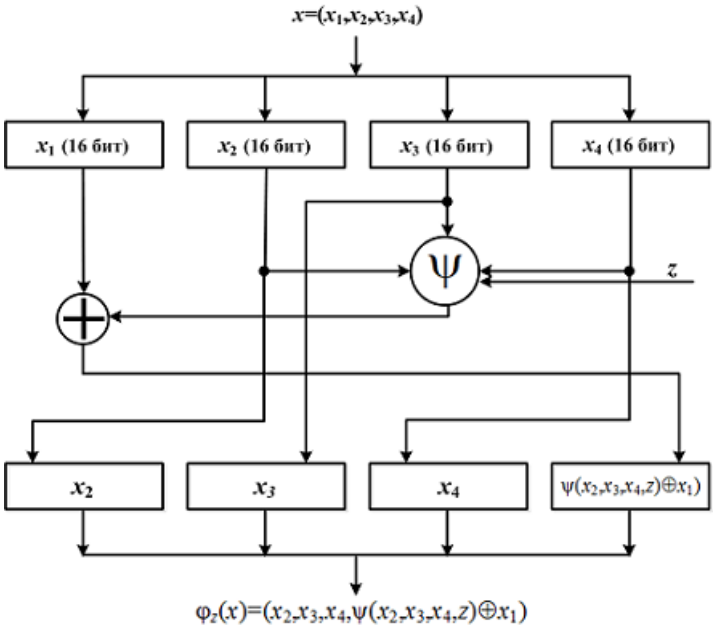

Рис. 1. Схема раундовой подстановки $\varphi_z(x)$

Подблоки ψ_2, ψ_3, ψ_4, кодирующие существенную зависимость выходных битов функции усложнения от битов векторов x_2,x_3,x_4, приведены на рис. 2.

0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0
1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1
0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0

Рис. 2. Вид подблоков ψ_2, ψ_3, ψ_4

Оценим характеристики перемешивающего графа подстановки $\varphi_z(x)$, используя [1].

Граф Γ_ψ с 16 вершинами является сильносвязным, что обеспечивается действием перестановки T^{11}. Следовательно, сильносвязным является и перемешивающий граф $\Gamma(\varphi)$.

Граф $\Gamma(\varphi)$ с 64 вершинами примитивен, что проверяется с помощью возведения в степень матрицы смежности вершин графа. Тогда при $n = 4$ и $r = 16$ верна оценка $\exp \Gamma_\psi \leqslant 312$.

Вместе с тем с помощью возведения в степень матрицы смежности вершин графа посчитано на ЭВМ точное значение экспонента перемешивающего графа: $\exp \Gamma(\varphi) = 7$. Большая разница между оценкой и точным значением экспонента объясняется большим разбросом значений экспонента и универсальностью оценки теоремы 3.3 [1].

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 α_0, α_1, α_2, α_3, $\alpha_5 < 2$, $\alpha_4 < 3$. Для данного уравнения введём обозначения для следующих переносов из младших n бит: