УДК 519.1 DOI 10.17223/2226308X/11/23

АНАЛИЗ СОВЕРШЕННОСТИ И СИЛЬНОЙ НЕЛИНЕЙНОСТИ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

А. Р. Мифтахутдинова

Экспериментально исследованы характеристики итеративных алгоритмов блочного шифрования с раундовой подстановкой на базе регистров сдвига (обобщение петли Фейстеля) из классов $R(8,32,3)$, $R(15,32,5)$, $R(16,32,5)$, $R(32,32,9)$ и $R(33,32,11)$, где $R(n,32,m)$ — класс автономных регистров сдвига длины n над множеством векторов V_{32} с m обратными связями (обобщение петли Фейстеля); $n > m \geqslant 1$; V_q — множество двоичных q-мерных векторов. Исследованы показатели совершенности и сильной нелинейности, определяемые как наименьшее число раундов, после которого произведение раундовых подстановок является совершенным и сильно нелинейным соответственно. Даны эмпирические оценки этих характеристик для некоторых алгоритмов из указанных классов. С использованием результатов сделаны рекомендации по числу раундов шифрования.

Ключевые слова: *сильная нелинейность, совершенность, экспонент графа.*

К шифрующим подстановкам блочных алгоритмов предъявляется ряд требований, направленных на обеспечение криптографической стойкости шифра. В частности, подстановка должна быть сильно нелинейной (то есть все её координатные функции не должны являться аффинными [1, с. 125]) и совершенной (то есть каждый бит выходного вектора должен существенно зависеть от всех битов входного вектора).

Шифрующая подстановка $g^{(h)}$ итеративного h-раундового алгоритма A блочного шифрования построена как произведение раундовых подстановок $g^{(h)} = p_1 \dots p_h$, где p_i — подстановка i-го раунда, $i = 1, \dots, h$. Показателем сильной нелинейности алгоритма A (обозначается $\operatorname{esn} A$) назовём наименьшее количество r раундов, при котором подстановка $g^{(r)}$ является сильно нелинейной; показателем совершенности алгоритма A (обозначается $\operatorname{epf} A$) назовём наименьшее количество r раундов, при котором подстановка $g^{(r)}$ является совершенной, $1 < r \leqslant h$. Заметим, что данные характеристики у алгоритма A могут не существовать.

Если перемешивающие орграфы раундовых подстановок совпадают и равны $\Gamma(g)$, то величина $\operatorname{epf} A$ оценивается снизу экспонентом орграфа $\Gamma(g)$ (обозначается $\exp \Gamma(g)$) [2, с. 101]. Величины $\operatorname{esn} A$ и $\operatorname{epf} A$ оцениваются сверху с помощью лемм 1 и 2 соответственно.

Обозначим: $I(x)$ — множество номеров единичных компонент вектора $x \in V_q$; g_j — j-я координатная функция подстановки g множества V_q, $j = 1, \dots, q$. Непосредственно из определений линейности булевой функции и существенной зависимости от переменной следуют леммы 1 и 2 соответственно.

Лемма 1. Пусть для некоторой четвёрки векторов a, b, c, ε из области определения раундовой подстановки g выполнено $g(a \oplus c) \oplus g(a) \oplus g(b \oplus c) \oplus g(b) = \varepsilon$, тогда функция g_j является нелинейной для любого $j \in I(\varepsilon)$.

Лемма 2. Пусть a и b — соседние по i-й координате векторы, $i = 1, \dots, q$, и для раундовой подстановки g выполнено $g(a) \oplus g(b) = \varepsilon$, тогда функция $g_j(x_1, \dots, x_q)$ существенно зависит от x_i для любого $j \in I(\varepsilon)$.

В ходе исследований были построены алгоритмы блочного шифрования с раундовой подстановкой на основе регистров сдвига из классов $R(8,32,3), R(15,32,5)$,

$R(16,32,5)$, $R(32,32,9)$ и $R(33,32,11)$. Из экспериментально проверенных соображений минимизации экспонента перемешивающего орграфа расположение обратных связей взято равноудалённое или близкое к нему, то есть расстояние между соседними точками съёма близко к n/m.

Приведём для примера h-раундовый алгоритм 512-5 из класса $R(16,32,5)$ (h — параметр). На i-м раунде шифрования реализуется подстановка g, зависящая от раундовых ключей $q_1^i,\ldots,q_5^i \in V_{32}$. Обозначим через $X=(X_0,\ldots,X_{15})$ входной блок раунда, $X_k \in V_{32}$, $0 \leqslant k \leqslant 15$. При ключах $q_1,\ldots,q_5$ раундовая подстановка множества V_{512} (рис. 1) задана формулой

$$g(X_0,\ldots,X_{15}) = (X_1, f(S,q_1)\boxplus X_2, X_3, X_4, f(S,q_2)\boxplus X_5, X_6, X_7, X_8, f(S,q_3)\boxplus X_9,$$
$$X_{10}, X_{11}, f(S,q_4)\boxplus X_{12}, X_{13}, X_{14}, f(S,q_5)\boxplus X_{15}, X_0),$$

где $S = X_0 \boxplus X_1 \boxplus X_3 \boxplus X_4 \boxplus X_6 \boxplus X_7 \boxplus X_8 \boxplus X_{10} \boxplus X_{11} \boxplus X_{13} \boxplus X_{14}$; $\boxplus$ — сложение по модулю 2^{32}. Функция f обратной связи совпадает с функцией алгоритма ГОСТ 28147-89.

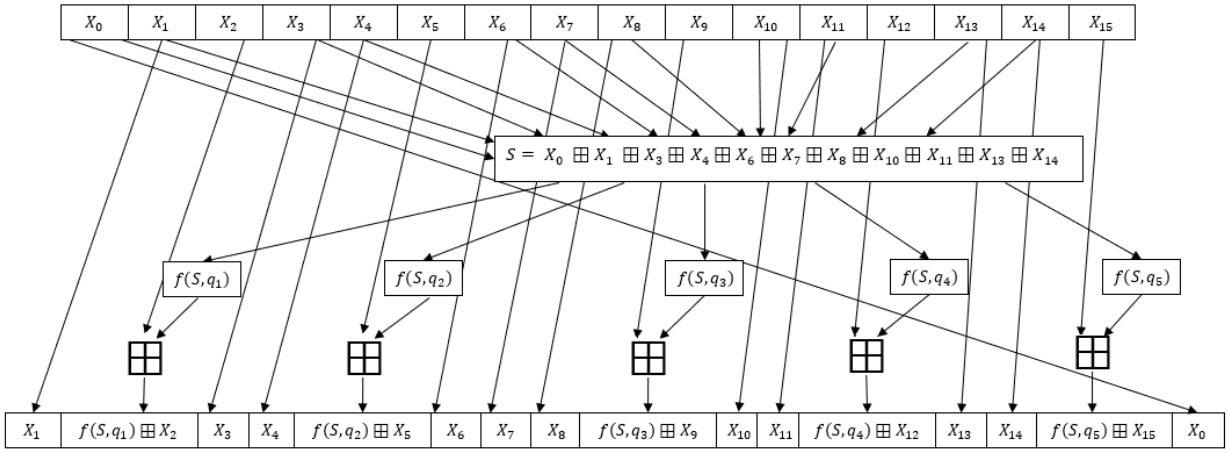

Рис. 1. Раундовая подстановка алгоритма 512-5

Для оценки показателя сильной нелинейности алгоритма 512-5 генерируем наборы случайных 512-мерных векторов $(a_t,b_t,c_t), t=1,2,\ldots$, и при $r=2,3,\ldots,h$ вычисляем $\varepsilon_t^{(r)} = g^{(r)}(a_t)\oplus g^{(r)}(b_t)\oplus g^{(r)}(a_t\oplus c_t)\oplus g^{(r)}(b_t\oplus c_t)$, $\varepsilon_t^{(r)} \in V_{512}$. Если при некотором t (из вероятностных соображений взято $t \leqslant 100$) вектор $\varepsilon_1^{(r)} \vee \ldots \vee \varepsilon_t^{(r)}$ (покоординатная дизъюнкция) состоит только из единиц, то $\operatorname{esn} A \leqslant r$.

Для оценки показателя совершенности алгоритма генерируем наборы случайных 512-мерных векторов, соседних по координате x_i, и при $r=2,3,\ldots,h$ вычисляем значение $\varepsilon_t^{(r)} = g^{(r)}(a_t)\oplus g^{(r)}(b_t)$, $\varepsilon_t^{(r)} \in V_{512}$. Если при некотором $t \leqslant 100$ результат покоординатной дизъюнкции векторов $\varepsilon_1^{(r)},\ldots,\varepsilon_t^{(r)}$ для $i=1,\ldots,512$ состоит только из единиц, то $\operatorname{epf} A \leqslant r$.

С помощью данных экспериментов оцениваем минимальное число раундов, необходимое для обеспечения сильной нелинейности и совершенности алгоритма шифрования. Если при опробовании 100 наборов векторов условие сильной нелинейности или совершенности не выполняется, то делается вероятностный вывод об отсутствии свойства сильной нелинейности и совершенности соответственно.

Для каждого алгоритма — представителя указанных классов вида $R(n,32,m)$ — проведено по 20 экспериментов, в ходе которых посчитан $\exp\Gamma(g)$ и получена оценка

показателей сильной нелинейности и совершенности (таблица). Во всех экспериментах полученные оценки совпали для каждого из рассмотренных блочных алгоритмов.

Оценки показателей сильной нелинейности и совершенности

n	m	$\exp\Gamma(g)$	$\operatorname{esn} A$	$\operatorname{epf} A$
8	3	4	3	7
15	5	4	3	7
16	5	7	4	8
32	9	7	4	8
33	11	4	3	6

Таким образом, при равноудалённом (или приблизительно равноудалённом) размещении обратных связей на регистре сдвига:

1) число раундов для достижения алгоритмом сильной нелинейности ($\operatorname{esn} A$) близко к величине n/m;
2) число раундов для достижения алгоритмом совершенности ($\operatorname{epf} A$) не меньше γ и не больше 2γ, где $\gamma = 2\exp\Gamma(g)$;
3) число раундов шифрования при синтезе шифров данного класса целесообразно установить не меньше $2\exp\Gamma(g)$.

ЛИТЕРАТУРА

1. *Фомичёв В. М., Мельников Д. А.* Криптографические методы защиты информации. Ч. 1. Математические аспекты: учебник для академического бакалавриата. М.: Юрайт, 2016. 209 с.
2. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.

УДК 519.7 DOI 10.17223/2226308X/11/24

ПРОПОЗИЦИОНАЛЬНОЕ КОДИРОВАНИЕ ПРЯМЫХ И ОБРАТНЫХ РАУНДОВЫХ ПРЕОБРАЗОВАНИЙ В АТАКАХ НА НЕКОТОРЫЕ БЛОЧНЫЕ ШИФРЫ[1]

И. В. Отпущенников, А. А. Семёнов, О. С. Заикин

Описывается атака на блочные шифры, основанная на известной концепции «встреча посередине». В рамках предлагаемой атаки для решения уравнений криптоанализа используются алгоритмы решения проблемы булевой выполнимости. Основное нововведение заключается в том, что в пропозициональной кодировке шифра учитывается информация не только от прямых, но и от обратных раундовых преобразований. Для ряда сокращённых по числу раундов блочных шифров построены оценки трудоёмкости атак из класса «угадывай и определяй» с использованием нового принципа кодирования. В некоторых случаях новые атаки оказались в разы эффективнее аналогов, в которых используются стандартные методы кодирования.

Ключевые слова: *блочный шифр, ГОСТ 28147-89, DES, PRESENT, криптоанализ, задача булевой выполнимости.*

[1]Работа поддержана грантом РНФ № 16-11-10046. Дополнительно И. В. Отпущенников поддержан Советом по грантам при Президенте РФ (стипендия № СП-4751.2016.5).