метода полиномиальная, если $y(1)$ не входит в ключ, и не превосходит 2^m в противном случае. Ключ $x(1)$ автомата A_1 находится решением его системы уравнений E_1, а вскрытие ключа f_1 в A_1, в свою очередь, сводится к доопределению частичной булевой функции со значениями $u(t)$ на состояниях $x(t)$ для $t = 1, 2, \ldots, l-1$ до функции в классе функции f_1. Аналогично, к доопределению частичной булевой функции со значениями $z(t)$ на парах $(u(t), y(t))$ для $t = 1, 2, \ldots, l$ до функции в классе функции f_2 сводится вскрытие ключа f_2 произвольного генератора G. Осуществление подобного доопределения демонстрируется на классе, состоящем из всех булевых функций от большого числа переменных с малым количеством существенных аргументов из них.

ЛИТЕРАТУРА

1. *Фомичёв В. М.* Дискретная математика и криптология. М.: ДИАЛОГ-МИФИ, 2003. 400 с.

УДК 519.7 DOI 10.17223/2226308X/9/18

О ГРУППЕ, ПОРОЖДЁННОЙ РАУНДОВЫМИ ФУНКЦИЯМИ АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ «КУЗНЕЧИК»

В. В. Власова, М. А. Пудовкина

Одно из направлений исследований итерационных алгоритмов блочного шифрования заключается в описании свойств группы, порожденной множеством всех частичных раундовых функций. Алгоритм «Кузнечик» является новым российским стандартом блочного шифрования. Доказывается, что группа, порождённая множеством всех частичных раундовых функций алгоритма блочного шифрования «Кузнечик», является знакопеременной.

Ключевые слова: *«Кузнечик», ГОСТ Р 34.12-2015, знакопеременная группа.*

Частичные раундовые функции многих алгоритмов блочного шифрования, появившихся в последние годы, представимы в виде композиции преобразований, реализующих слой наложения ключа (X-слой), слой s-боксов (S-слой) и линейный слой (L-слой). Такие алгоритмы называются XSL-алгоритмами блочного шифрования. XSL-алгоритмом является американский стандарт блочного шифрования AES и российский стандарт блочного шифрования «Кузнечик», вступивший в силу в январе 2016 г. Групповым свойствам XSL-алгоритмов посвящены работы [1 – 4]. В [1] для алгоритма AES доказывается, что группа G, порождённая всеми частичными раундовыми функциями, совпадает со знакопеременной. В [3] получены условия, достаточные для примитивности группы G XSL-алгоритма, и доказано, что AES удовлетворяет данным условиям. В [4, 2] получены достаточные условия того, что группа G XSL-алгоритма равна знакопеременной. В [5] приведено исследование приложения группового подхода к построению и анализу криптографических систем.

В данной работе доказывается, что группа, порождённая множеством всех частичных раундовых функций алгоритма «Кузнечик», совпадает со знакопеременной. Для этого используется теорема 1 из [2].

Рассмотрим итерационный алгоритм блочного шифрования. Частичная r-раундовая функция шифрования f_k представима в виде композиции r частичных раундовых функций $g_{k_1}, \ldots, g_{k_r}$, где k_i — раундовый ключ из множества ключей шифрования i-го раунда $K^{(i)}$, $i = 1, \ldots, r$. Во многих алгоритмах множества раундовых ключей совпадают, потому далее в тексте $K^{(1)} = \ldots = K^{(r)} = K$. В работе рассматривается группа $G = \langle g_k \mid k \in K \rangle$.

Обозначим V_l — l-мерное векторное пространство над полем $\mathrm{GF}(2)$; $S(V_l)$ и $A(V_l)$ — соответственно симметрическая и знакопеременная группы, действующие на пространстве V_l; $+$ — операция покоординатного сложения по модулю 2 двоичных векторов. В рассматриваемом алгоритме блочного шифрования блоки текстов из множества V_{mn} представимы также как векторы из декартова произведения ${V_n}^m$, $m > 1$ и $n > 1$ — натуральные числа. Данные представления отождествляются.

Частичная раундовая функция $g_k : V_{mn} \to V_{mn}$ задана условием

$$g_k : (x_1, \ldots, x_n) \mapsto a(s_1(x_1 + k^{(1)}), \ldots, s_n(x_n + k^{(n)})),$$

где $k = (k^{(1)}, \ldots, k^{(n)})$ — раундовый ключ; $x_i, k^{(i)} \in V_m$; подстановки (s-боксы) $s_1, \ldots, s_n \in S(V_m)$ действуют на V_m; a — линейное преобразование из полной линейной группы преобразований пространства V_{mn}.

Приведём достаточные условия для выполнения равенства $G = \langle g_k \mid k \in K \rangle = A(V_{mn})$.

Линейному преобразованию $a : {V_n}^m \to {V_n}^m$ поставим в соответствие орграф $\Gamma(a)$ с множествами вершин $\{1, \ldots, n\}$ и дуг X, в котором дуга $(i, j) \in X$ тогда и только тогда, когда j-я координатная функция $a_j(x_1, \ldots, x_n)$ линейного преобразования a существенно зависит от x_i, где $x_1, \ldots, x_n \in V_m$.

Вектору $x = (x_1, \ldots, x_n) \in {V_n}^m$, поставим в соответствие множество $I(x) = \{i \in \{1, \ldots, n\} : x_i \neq 0_m\}$, где 0_m — нулевой вектор пространства V_m. Если I — подмножество вершин графа $\Gamma(a)$, то $J(I)$ — множество концов дуг с началом в множестве I.

Подстановке s_i поставим в соответствие подстановки

$$s_{i,k,k'} : x \mapsto s_i^{-1}(k' + s_i(x + k)),$$

где $k, k' \in V_m$, $i = 1, \ldots, n$. Обозначим через $H(s_i) = \langle s_{i,k,k'} \mid (k, k') \in V_m^2 \rangle$ порождённую данными подстановками группу.

Теорема 1 [2]. Пусть выполнены следующие условия:

1) граф $\Gamma(a)$ является примитивным;
2) для любого множества $L \subseteq \{1, \ldots, n\}$ выполнено неравенство

$$\max_{\{x \in V_{mn} : I(x) = L\}} |I(a(x))| \geqslant |L|;$$

3) группы $H(s_1), \ldots, H(s_n)$ являются 2-транзитивными и среди элементов данных групп существует такая подстановка $s \in S(V_m)$, что

$$|\{x \in V_m : s(x) = x\}| \notin \{0, 2^0, 2^1, 2^2, \ldots, 2^m\}.$$

Тогда $G = \langle g_k \mid k \in K \rangle = A(V_{mn})$.

Проверим выполнение данных условий для алгоритма блочного шифрования «Кузнечик» [6].

Для проверки условия 1 теоремы 1 рассмотрим свойства линейного преобразования a алгоритма «Кузнечик». Путём непосредственных вычислений найден орграф $\Gamma(a)$. Известно [7], что граф примитивен тогда и только тогда, когда он сильно связен и наибольший общий делитель длин всех его простых контуров равен 1. Экспериментально проверено выполнение условий, достаточных для примитивности орграфа $\Gamma(a)$.

Проверка условия 2 теоремы 1 осуществлялась с помощью [2, теорема 2], согласно которой условие 2 выполняется, в частности, если выполнено неравенство

$$2^{mn} < (2^m - 1)^{n-1}(2^m + 2^{m-1} - 2). \tag{1}$$

Справедливость неравенства (1) проверена с помощью непосредственных вычислений (левая часть неравенства (1) равна $3{,}4028 \cdot 10^{38}$, правая часть — $4{,}7881 \cdot 10^{38}$).

Для проверки условия 3 теоремы 1 найдена разностная матрица λ s-боксов алгоритма «Кузнечик». Данной матрице поставлен в соответствие граф $\Lambda(s_i)$, определяемый матрицей смежности $\lambda(s_i)\lambda(s_i)^{\mathrm{T}} = (m_{\alpha\beta})$, где $\lambda(s_i)^{\mathrm{T}}$ — транспонированная матрица $\lambda(s_i)$. Множеством вершин графа $\Lambda(s_i)$ является множество всех ненулевых векторов из V_m, вершины α и β соединены ребром тогда и только тогда, когда $m_{\alpha\beta} > 0$.

Согласно [2, теорема 3], для 2-транзитивности группы $H(s_i)$ необходима и достаточна связность графа $\Lambda(s_i)$. Экспериментально проверена связность графа $\Lambda(s_i)$ для s-боксов алгоритма «Кузнечик».

Выполнение второй части условия 3 теоремы 1 эквивалентно нахождению в разностной матрице s-боксов алгоритма «Кузнечик» элементов, отличных от степеней 2. Непосредственно проверено существование таких элементов в разностной матрице λ.

Теорема 2. Для алгоритма блочного шифрования «Кузнечик» группа G, порождённая множеством всех частичных раундовых функций, равна знакопеременной группе $A(V_{128})$.

ЛИТЕРАТУРА

1. *Wernsdorf R.* The round functions of RIJNDAEL generate the alternating group // LNCS. 2002. V. 2365. P. 143–148.
2. *Маслов А. С.* Об условиях порождения SA-подстановками знакопеременной группы // Труды института математики. 2007. Т. 15. № 2. С. 58–68.
3. *Caranti A., Dalla Volta F., Sala M., and Villani F.* Imprimitive permutation groups generated by the round functions of key-alternating block ciphers and truncated differential cryptanalysis. `http://arxiv.org/pdf/math/0606022.pdf`
4. *Caranti A., Dalla Volta F., and Sala M.* An application of the O'Nan-Scott theorem to the group generated by the round functions of an AES-like cipher // Designs, Codes and Cryptography. 2009. V. 52. P. 293–301.
5. *Глухов М. М., Погорелов Б. А.* О некоторых применениях групп в криптографии // Математика и безопасность информационных технологий. Материалы конф. в МГУ 28–29 октября 2004. М.: МЦНМО, 2005. С. 19–31.
6. ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры. М.: Стандартинформ, 2015.
7. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.