УДК 621.391: 519.7

А. Н. Алексейчук
Специальный факультет СБ Украины в составе Военного института телекоммуникаций и информатизации НТУУ «КПИ»
ул. Московская, 45/1, 01011 Киев, Украина

Критерий примитивности группы подстановок, порожденной раундовыми преобразованиями Rijndael-подобного блочного шифра

Рассмотрена алгебраическая модель Rijndael-подобного блочного шифра, s-блоки которого имеют тривиальную линейную структуру. Получены необходимые и достаточные условия, при которых раундовые шифрующие преобразования данного шифра порождают примитивную группу подстановок, что исключает возможность проведения на шифр ряда известных алгебраических атак. Показано, что группа, порожденная раундовыми преобразованиями шифра Rijndael, является примитивной.

Ключевые слова: *криптографическая защита информации, блочный шифр, примитивная группа подстановок, Rijndael.*

Одной из важных задач, связанных с повышением информационной безопасности современных телекоммуникационных систем, является совершенствование криптографических методов и средств защиты информации, циркулирующей в этих системах. К таким средствам относятся, в частности, блочные шифры (БШ), широко используемые в автоматизированных системах обработки данных для обеспечения конфиденциальности передаваемой или хранимой информации.

При изучении криптографических свойств блочных шифров, не связанных с особенностями их технической (программной) реализации или процессами функционирования соответствующих шифрующих устройств, как правило, используются две основные математические модели БШ: алгебраическая и вероятностная [1, 2]. В настоящей статье рассматривается алгебраическая модель блочно-итерационного шифра, формальное описание которой приведено ниже.

Пусть даны конечная абелева группа G, непустые конечные множества K, Λ и семейство $(f_k: G^n \to G^n, k \in K)$ взаимно однозначных преобразований множества $G^n = \{(g_1, \ldots, g_n): g_i \in G, i \in \overline{1,n}\}$. Согласно определению [1], r-раундовый блочно-итерационный шифр $\Im$ с множеством открытых (шифрованных) сообщений G^n, множеством ключей Λ, множеством тактовых ключей K, расписанием ключей

θ: $\Lambda \to K^r$ и функцией шифрования F: $G^n \times \Lambda \to G^n$ представляет собой систему (G^n, Λ, K, F, θ) такую, что для любых $x \in G^n$, $\lambda \in \Lambda$ выполняется равенство

$$F(x, \lambda) = f_{k(r)} \dots f_{k(1)}(x),$$

где $(k(1), \dots, k(r)) = \theta(\lambda)$ и $f_{k(r)} \dots f_{k(1)}$ есть произведение (последовательное выполнение) указанных преобразований. Элементы $k(1), \dots, k(r)$ называются тактовыми ключами, а отображения $f_{k(1)}, \dots, f_{k(r)}$ — раундовыми шифрующими преобразованиями шифра $\mathfrak{I}$ в тактах (раундах) шифрования с номерами 1, …, r соотвественно.

Как правило, при анализе стойкости данного блочного шифра $\mathfrak{I}$ относительно криптоаналитических атак, не использующих конкретные особенности расписания ключей θ, в приведенном выше определении полагают $\Lambda = K^r$, $\theta(\lambda) = \lambda = (k(1), \dots, k(r))$, т.е. считают, что последовательность тактовых ключей может быть произвольным элементом множества K^r. В дальнейшем это соглашение принимается в настоящей статье.

Одним из общих требований к современным блочным шифрам является их обоснованная стойкость относительно алгебраических методов криптоанализа, основанных на группировании открытых, шифрованных сообщений или ключей шифра в классы эквивалентных (или близких, в том или ином смысле) объектов, позволяющем понизить трудоемкость алгоритмов решения соответствующих криптоаналитических задач. Стойкость БШ к подобным методам криптоанализа, получившим в ряде публикаций название методов гомоморфных образов или гомоморфизмов [2–4], как правило, определяется алгебраическими свойствами различных групп подстановок, связанных с системой раундовых преобразований данного блочного шифра $\mathfrak{I}$.

Обозначим через $G(\mathfrak{I}) = < f_k : k \in K >$ подгруппу симметрической группы множества G^n, порожденную подстановками f_k: $G^n \to G^n$, $k \in K$. Напомним [5], что группа $G(\mathfrak{I})$ называется транзитивной, если для любых $x, y \in G^n$ существует подстановка $g \in G(\mathfrak{I})$ со свойством $g(x) = y$. Транзитивная группа $G(\mathfrak{I})$ называется импримитивной, если она имеет нетривиальный блок (т.е. такое множество $\Delta \subseteq G^n$, что $1 < |\Delta| < |G^n|$, и для любого $g \in G(\mathfrak{I})$ выполняется одно из условий $g(\Delta) = \Delta$, $g(\Delta) \cap \Delta = \varnothing$), и примитивной — в противном случае.

Изучению взаимосвязи между криптографической стойкостью шифра $\mathfrak{I}$ и свойствами группы $G(\mathfrak{I})$ посвящены статьи [6–10] и ряд других работ. В частности, в [6, 7, 10] показано, что необходимым условием стойкости шифра $\mathfrak{I}$ к определенным алгебраическим атакам на основе известных или подобранных открытых сообщений является выполнение следующих требований:

1) группа $G(\mathfrak{I})$ примитивна;

2) эта группа имеет достаточно большой порядок (например, такой, при котором исключена возможность практического перечисления всех шифрующих преобразований $F_\lambda = f_{k(r)} \dots f_{k(1)}$, $\lambda \in \Lambda$ в r раундах шифрования).

В [6] показано также, что импримитивность группы $G(\mathfrak{I})$ может свидетельствовать о наличии в конструкции шифра $\mathfrak{I}$, так называемых «потайных лазеек», существенно снижающих его практическую стойкость. В доказательство этого в [6] приводится пример 32-раундового шифра с длинами блока и ключа шифрова-

ния, равными соответственно 64 и 80 битам. Этот шифр по своей структуре аналогичен алгоритму DES, за исключением конструкции *s*-блоков, и, как показано в [6], является практически стойким к линейному и разностному криптоанализу. Вместе с тем, импримитивность группы данного шифра позволяет осуществить на него алгебраическую атаку с использованием 2^{32} подобранных открытых текстов.

Необходимо отметить, что на практике вычисление группы, порожденной раундовыми шифрующими преобразованиями данного блочного шифра $\Im$, как правило, представляет собой достаточно трудную задачу, которая становится практически неразрешимой при отсутствии полной информации о криптографической схеме шифра. В этом случае скрытые в конструкции шифра «лазейки», основанные на импримитивности указанной группы подстановок, практически не удается обнаружить [6]. Таким образом, установление факта примитивности группы $G(\Im)$ является первым шагом на пути обоснования стойкости шифра $\Im$ к алгебраическим атакам и отсутствия в конструкции этого шифра определенных скрытых «лазеек».

Целью настоящей статьи является доказательство теоремы, устанавливающей необходимые и достаточные условия примитивности группы подстановок, порожденной раундовыми преобразованиями Rijndael-подобного блочного шифра [11]. (Эти шифры получили свое название в честь нового американского стандарта шифрования данных, утвержденного в США в 2001 году [12]). Приведенные ниже условия примитивности группы $G(\Im)$ допускают простую алгоритмическую проверку; в частности, с их помощью нетрудно показать, что раундовые преобразования шифра Rijndael порождают примитивную группу подстановок.

Приведем точные определения основных понятий, используемых в дальнейшем изложении. Рассмотрим блочный шифр $\Im = (G^n, \Lambda, K, F, \theta)$ над алфавитом G^n, где G является аддитивной группой конечного поля порядка $q = 2^l$, $\Lambda = K^r$ и $K = G^n$.

Шифр $\Im$ называется Rijndael-подобным [11], если существуют подстановки $s_1, \ldots, s_n$ на множестве G и невырожденное линейное преобразование M векторного пространства G^n над полем $\mathbf{GF}(q)$ такие, что для любого $k \in K$ шифрующее преобразование f_k в каждом из r раундов имеет вид

$$f_k(x) = f(x + k),\ x \in G^n, \tag{1}$$

где

$$f(x) = Ms(x) = M(s_1(x_1), \ldots, s_n(x_n))^T,\ x = (x_1, \ldots, x_n) \in G^n. \tag{2}$$

Отображение f: $G^n \to G^n$, определяемое по формуле (2), называется раундовой функцией шифра $\Im$, а подстановки s_i ($i \in \overline{1, n}$) — s-блоками этого шифра.

В дальнейшем линейное преобразование M отождествляется с квадратной матрицей порядка n над полем $\mathbf{GF}(q)$. В этом случае запись $Ms(x)$ в выражении (2) обозначает результат умножения вектор-столбца $s(x)$ длины n на матрицу M; аналогичное соглашение действует относительно умножения матриц на вектор-строки.

Введем ряд вспомогательных понятий. Следуя [13], назовем матрицу A порядка n над полем $\mathbf{GF}(q)$ разложимой, если существуют натуральное число k, $1 \le k < n$, и подстановочная матрица P такие, что

$$A = P^{-1}\begin{pmatrix} A_1 & 0 \\ A_2 & A_3 \end{pmatrix}P,$$

где A_1 — матрица порядка k над полем $\mathbf{GF}(q)$. Матрица A, не являющаяся разложимой, называется неразложимой.

Обозначим через χ нетривиальный аддитивный характер поля $\mathbf{GF}(q)$ [5]. Для любой подгруппы L абелевой группы G^n символом $L^\perp$ обозначим подгруппу, дуальную к L: $L^\perp = \{x \in G^n: \chi(xy) = 1$ для любого $y \in L\}$ (напомним, что в соответствии с принятым выше соглашением запись xy обозначает скалярное произведение векторов x и y над полем из q элементов).

Рассмотрим произвольное отображение s: $\mathbf{GF}(q) \to \mathbf{GF}(q)$. Будем говорить, что s имеет тривиальную линейную структуру, если не существует элементов $a, b \in \mathbf{GF}(q) \setminus 0$ таких, что функция $\chi(bs(x + a) + bs(x))$, $x \in \mathbf{GF}(q)$ является константной. Отметим, что тривиальность линейной структуры каждого s-блока данного блочного шифра $\mathfrak{I}$, определяемого с помощью соотношений (1), (2), является одним из стандартных необходимых условий стойкости этого шифра к линейному криптоанализу [14, 15]. Известно, например [16], что этому условию удовлетворяют s-блоки шифра Rijndael.

Основной результат настоящей статьи содержит следующая теорема.

Теорема. Пусть $\mathfrak{I}$ — Rijndael-подобный блочный шифр, раундовые шифрующие преобразования которого определяются по формулам (1), (2). Предположим далее, что s-блоки $s_1, \ldots, s_n$ шифра $\mathfrak{I}$ имеют тривиальную линейную структуру. Тогда группа $G(\mathfrak{I})$ является примитивной в том и только том случае, когда матрица M неразложима.

Доказательство. Заметим, прежде всего, что блоки импримитивности группы $G(\mathfrak{I})$ являются также блоками импримитивности группы подстановок $< (f_{k_1})^{-1} f_{k_2} : k_1, k_2 \in K >$, которая в силу равенства (1) совпадает с группой сдвигов абелевой группы G^n. Отсюда следует (см., например, [5]), что каждая система блоков импримитивности группы $G(\mathfrak{I})$ является системой смежных классов группы G^n по некоторой ее подгруппе.

Предположим теперь, что $G(\mathfrak{I})$ — импримитивная группа подстановок и L — нетривиальный блок этой группы, содержащий нулевой вектор (нейтральный элемент группы G^n). Тогда L является собственной подгруппой группы G^n, и на основании равенства (1) и определения дуальной подгруппы для любых векторов $a = (a_1, \ldots, a_n) \in L$, $b = (b_1, \ldots, b_n) \in L^\perp$, $x = (x_1, \ldots, x_n) \in G^n$ выполняется равенство

$$\chi(bf(x + a) + bf(x)) = 1. \qquad (3)$$

Положим $L' = \{bM: b \in L^\perp\}$. Из равенств (2), (3) следует, что

$$\prod_{i=1}^{n} \chi(c_i s_i(x_i + a_i) + c_i s_i(x_i)) = 1$$

для любых $a = (a_1, \ldots, a_n) \in L$, $c = (c_1, \ldots, c_n) \in L'$, $x = (x_1, \ldots, x_n) \in G^n$, откуда, в свою очередь, вытекает тождество

$$\chi(c_i s_i(x_i + a_i) + c_i s_i(x_i)) \equiv \text{const}, x_i \in \mathbf{GF}(q), \qquad (4)$$

справедливое для всех $a \in L$, $c \in L'$, $i \in \overline{1,n}$.

Итак, на основании соотношений (4) и условия теоремы для любых $a \in L$, $c \in L'$, $i \in \overline{1,n}$ неравенство $a_i \neq 0$ ($c_i \neq 0$) влечет равенство $c_i = 0$ ($a_i = 0$). Отсюда вытекает, что $\chi(ca) = \chi(0) = 1$ для всех $a \in L$, $c \in L'$, и, следовательно, $L' \subseteq L^{\perp}$. Поскольку M является невырожденным линейным преобразованием, то множества L' и $L^{\perp}$ имеют одинаковую мощность. Следовательно, $L' = L^{\perp}$, и подгруппа $L^{\perp}$ инвариантна относительно преобразования M.

Положим $I_L = \{ i \in \overline{1,n} : a_i = 0$ для любого $a \in L\}$, $k = |I_L|$. Заметим, что $1 \le k < n$, так как L является нетривиальным блоком группы $G(\mathfrak{I})$. Перенумеруем координаты векторов, принадлежащих группе G^n, таким образом, чтобы выполнялось равенство $I_L = \{1, 2, \ldots, k\}$. Из определения дуальной подгруппы следует, что для любого $a = (a_1, \ldots, a_n) \in L$

$$L^{\perp}(a) \stackrel{\text{def}}{=} \{(c_1, \ldots, c_n) \in G^n : c_1, \ldots, c_k \in G^k, \chi(c_{k+1}a_{k+1} + \ldots + c_n a_n) = 1\} \subseteq L^{\perp}.$$

Если при этом $c_i \neq 0$ для некоторых $(c_1, \ldots, c_n) \in L^{\perp}(a)$, $i \in \overline{k+1,n}$, то, согласно полученному выше равенству $L^{\perp} = L'$, имеет место соотношение $i \in I_L$, что противоречит определению множества I_L. Таким образом,

$$L^{\perp} = \{(c_1, \ldots, c_n) \in G^n : c_1, \ldots, c_k \in G^k, c_{k+1} = \ldots = c_n = 0\}, \qquad (5)$$

в частности, подгруппа $L^{\perp}$ является подпространством векторного пространства $\mathbf{GF}(q)^n$ над полем $\mathbf{GF}(q)$. Наконец, так как собственное инвариантное относительно матрицы M подпространство $L^{\perp}$ имеет вид (5), то M является разложимой матрицей, что и требовалось доказать.

Предположим теперь, что матрица M разложима и покажем, что $G(\mathfrak{I})$ — импримитивная группа. Перенумеровав подходящим образом строки и столбцы матрицы M, представим эту матрицу в виде

$$M = \begin{pmatrix} M_1 & 0 \\ M_2 & M_3 \end{pmatrix}, \qquad (6)$$

где M_1 — матрица порядка k над полем $\mathbf{GF}(q)$, $1 \le k < n$. Несложная проверка показывает, что подпространство $L^{\perp}$ вида (5) инвариантно относительно матрицы M

вида (6), и для любых $a \in L = \{(c_1, \ldots, c_n) \in G^n: c_1, \ldots, c_k = 0, c_{k+1} = \ldots = c_n \in G^{n-k}\}$, $b \in L^{\perp}$, $x \in G^n$ выполняется равенство (3). Отсюда вытекает, что множество L является нетривиальным блоком группы $G(\mathfrak{I})$ и, следовательно, $G(\mathfrak{I})$ — импримитивная группа подстановок. Теорема доказана.

Непосредственно из утверждения полученной теоремы и известного критерия неприводимости линейного преобразования над полем (см., например, [5], гл. XV, теор. 14) вытекает следующий результат.

Следствие 1. В условиях доказанной выше теоремы $G(\mathfrak{I})$ является примитивной группой, если характеристический многочлен матрицы M неприводим над полем $\mathbf{GF}(q)$. В частности, если M — полноцикловое линейное преобразование векторного пространства $\mathbf{GF}(q)^n$, то $G(\mathfrak{I})$ — примитивная группа подстановок.

Отметим, что на практике проверить разложимость или неразложимость данной квадратной матрицы M можно с использованием известных алгоритмов, изложенных, например, в [13]. Приведем здесь простое достаточное условие неразложимости матрицы M, позволяющее с помощью несложной проверки убедиться в том, что группа подстановок, порожденная раундовыми преобразованиями шифра Rijdael, является примитивной.

Обозначим через $B = \left\| b_{ij} \right\|_{n \times n}$ носитель матрицы $M = \left\| m_{ij} \right\|_{n \times n}$, т.е. вещественную (0, 1)-матрицу с элементами $b_{ij} = 1$, если $m_{ij} \neq 0$; $b_{ij} = 0$ — в противном случае, $i, j \in \overline{1, n}$. Согласно [13], матрица M является неразложимой, если сушествует натуральное t, для которого все элементы t-й степени матрицы B — положительные вещественные числа.

В качестве применения полученных результатов, рассмотрим шифр Rijdael с длиной блока шифруемого сообщения, равной 128 битам (варианты шифрования блоков длины 192 бита или 256 бит рассматриваются аналогично). В этом случае в выражениях (1), (2) $G = (\mathbf{GF}(2^8), +)$, $n = 16$, и M является произведением двух матриц 16-го порядка над полем из 2^8 элементов:

$$M = \operatorname{diag}(D, D, D, D)\, \Pi_{16}, \tag{7}$$

где D — матрица порядка 4 над полем $\mathbf{GF}(2^8)$, все элементы которой отличны от 0, Π_{16} — подстановочная матрица, соответствующая подстановке на множестве $\{0, 1\}^{16}$, преобразующей двоичный вектор $(x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10}, x_{11}, x_{12}, x_{13}, x_{14}, x_{15})$ в вектор $(x_0, x_{13}, x_{10}, x_7, x_4, x_1, x_{14}, x_{11}, x_8, x_5, x_2, x_{15}, x_{12}, x_9, x_6, x_3)$ [12]. Несложная проверка показывает, что носитель B матрицы M имеет следующий вид:

$$B = \begin{pmatrix} e_4 000 & 000 e_4 & 00 e_4 0 & e_4 00 0 \\ 0 e_4 0 0 & e_4 000 & 000 e_4 & 00 e_4 0 \\ 00 e_4 0 & 0 e_4 00 & e_4 000 & 000 e_4 \\ 000 e_4 & 00 e_4 0 & 0 e_4 00 & 0 e_4 00 \end{pmatrix}, \tag{8}$$

где $e_4 = (1, 1, 1, 1)^T$ и $0 = (0, 0, 0, 0)^T$ — вектор-столбцы длины 4, состоящие из единиц и нулей соответственно. Используя соотношение (8), нетрудно убедиться в том, что все элементы матрицы B^2 положительны. Следовательно, матрица M вида (7) является неразложимой.

Итак, справедливо следующее утверждение.

Следствие 2. Раундовые преобразования шифра Rijdael порождают примитивную группу подстановок.

В плане дальнейших исследований, отметим, прежде всего, задачи вычисления или оценки значений различных числовых параметров [17], связанных с группами, порожденными раундовыми преобразованиями Rijdael-подобных блочных шифров. Несомненный практический интерес представляет также ответ на вопрос о том, совпадает ли группа, порожденная раундовыми преобразованиями шифра Rijdael, с симметрической или знакопеременной группой подстановок на множестве блоков шифруемых сообщений.

1. *Харин Ю.С., Берник В.И., Матвеев Г.В.* Математические основы криптологии. — Минск: Изд-во БГУ, 1999. — 319 с.

2. *Бабаш А.В., Шанкин Г.П.* Криптография. — М.: Солон-Р, 2002. — 511 с.

3. *Горчинский Ю.Н.* О гомоморфизмах многоосновных универсальных алгебр в связи с криптографическими применениями // Труды по дискретной математике. — Т. 1. — М.: ТВП, 1997. — С. 67–84.

4. *Шапошников И.Г.* О конгруэнциях конечных многоосновных универсальных алгебр // Дискретная математика. — 1999. — Т. 11. — Вып. 3. — С. 48–62.

5. *Глухов М.М., Елизаров В.П., Нечаев А.А.* Алгебра: Учебник. В 2-х т. Т.II. — М.: Гелиос АРВ, 2003. — 416 с.

6. *Paterson K.G.* Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers // Fast Software Encryption. — FSE'99, Proceedings. — Springer Verlag, 1999. — P. 201–214.

7. *Campbell K.W., Wiener M.* DES is Not a Group // Advances in Cryptology — CRYPTO'92, Proceedings. — Springer Verlag, 1993. — P. 512–520.

8. *Even S., Goldreich O.* DES-Like Functions Can Generate the Alternating Group // IEEE Trans. on Information Theory. — 1983. — V. 29. — P. 863–865.

9. *Hornauer G., Stephan W., Wernsdorf R.* Markov ciphers and alternating groups // Advances in Cryptology — EUROCRYPT'93, Proceedings. — Springer Verlag, 1994. — P. 453–460.

10. *Kaliski B.S., Rivest R.L., Sherman A.T.* Is the Data Encryption Standard a Group? (Results of Cycling Experiments on DES) // J. Cryptology. — 1988. — №. 1. — P. 3–36.

11. *Park S., Sung S.H., Chee E-J. J., Lim J.* On the Security of Rijndael-Like Structures Against Differential and Linear Cryptanalysis // Advances in Cryptology — ASIACRYPT'02, Proceedings. — Springer Verlag, 2002. — P. 176–191.

12. *Daemen J., Rijmen D.* AES Proposal: Rijndael. htpp://csrc.nist.gov/encription/aes/rijndael/Rijndael.pdf.

13. *Сачков В.Н., Тараканов В.Е.* Комбинаторика неотрицательных матриц. — М.: ТВП, 2000. — 447 с.

14. *Chabaud F., Vaudenay S.* Links Between Differential and Linear Cryptanalysis // Advances in Cryptology — EUROCRYPT' 94, Proceedings. — Springer Verlag, 1995. — P. 356–365.

15. *Canteaut A.* Cryptographic Functions and Design Criteria for Block Ciphers // Advances in Cryptology — INDOCRYPT'2001, Proceedings. — Springer Verlag, 2001. — P. 1–16.

16. *Keliher L., Meier H., Tavares S.* Improving the Upper Bond on the Maximum Average Linear Hull Probability for Rijndael // Selected Areas in Cryptography. — SAC 2001. — Proceedings. — Springer Verlag, 2001. — P. 112–128.

17. *Глухов М.М.* О числовых параметрах, связанных с заданием конечных групп системами образующих элементов // Труды по дискретной математике. — Т. 1. — М.: ТВП, 1997. — С. 43–66.

Поступила в редакцию 22.03.2004