УДК 519.7

О ПРИМИТИВНОСТИ ПЕРЕМЕШИВАЮЩЕЙ МАТРИЦЫ ГЕНЕРАТОРА (δ, τ) -САМОУСЕЧЕНИЯ

Я. Э. Авезова, В. М. Фомичев

Получены условия примитивности перемешивающей матрицы генератора (δ, τ) -самоусечения и его обобщения, построенного на основе нелинейных подстановок векторного пространства над конечным полем. Даны верхние оценки экспонентов указанной перемешивающей матрицы.

Ключевые слова: генератор (δ, τ) -самоусечения, примитивный граф, примитивная матрица, экспонент матрицы.

Введение

Для генератора (δ, τ) -самоусечения, относящегося к классу генераторов с неравномерным движением [1, 2], известны результаты, связанные с длиной периода и линейной сложностью вырабатываемой гаммы. Работа посвящена перемешивающим свойствам преобразования состояний генератора (δ, τ) -самоусечения и его обобщения, построенного на основе нелинейных подстановок векторного пространства над конечным полем.

Пусть генератор (δ, τ) -самоусечения построен на основе регистра сдвига (не обязательно линейного) длины n над конечным полем P . Обозначим через h базовое преобразование (пространства P^n) генератора и через H — квадратную матрицу порядка n , являющуюся перемешивающей матрицей преобразования h . Если x — состояние регистра и знак управляющей гаммы равен 1 (в частности, состояние некоторой ячейки регистра), то выполняется преобразование $h^\delta(x)$. Если знак управляющей гаммы равен 0, то выполняется преобразование $h^\tau(x)$. Следовательно, перемешивающая матрица преобразования состояний регистра равна $H^\delta + H^\tau$.

Предмет исследования — примитивность матрицы $H^\delta + H^\tau$ и величина $\exp(H^\delta + H^\tau)$.

Графом 0,1-матрицы называется орграф $\Gamma(A)$, у которого матрица смежности вершин есть A .

Теорема 1.

- 1) Если матрица H примитивная и $\exp H = t$, то матрица $H^\delta + H^\tau$ также примитивная и $\exp(H^\delta + H^\tau) \leq \lceil t/\tau \rceil$.
- 2) Если матрица H не примитивная и $\{l_1, \dots, l_m\}$ есть множество всех длин простых контуров орграфа $\Gamma(H)$, где $(l_1, \dots, l_m) = d > 1$, то матрица $H^\delta + H^\tau$ примитивна, если τ кратно d и $(\delta, l_i) = 1, i = 1, \dots, m$.
- 3) Пусть в условиях п. 2 число τ кратно d , $\mu_i = l_i/(\tau, l_i), i = 1, \dots, m$, и $\{\lambda_1, \dots, \lambda_r\}$ есть множество различных чисел среди $\mu_1, \dots, \mu_m$, где $r \leq m$ и $\lambda_1 < \dots < \lambda_r$. Тогда:
 - а) если $\lambda_1 > 1$ и $r > 2$, то

$$\exp(H^\delta + H^\tau) \leq g(\lambda_1, \dots, \lambda_r) + n(r + 1) - \sum_{i=1}^r \lambda_i,$$

где $g(\lambda_1, \dots, \lambda_r)$ — число Фробениуса от аргументов $\lambda_1, \dots, \lambda_r$, то есть наибольшее натуральное число, не принадлежащее аддитивной полугруппе, порождённой натуральными числами $\lambda_1, \dots, \lambda_r$;

б) если $\lambda_1 > 1$ и $r = 2$, то

$$\exp(H^\delta + H^\tau) \leq \lambda_1 \lambda_2 - 2\lambda_1 - \lambda_2 + 2n;$$

в) если $\lambda_1 = 1$ и μ — наибольшее число, делящее τ , среди чисел $l_1, \dots, l_m$, то

$$\exp(H^\delta + H^\tau) \leq 2n - 1 - \mu.$$

Оценки пп. 3б и 3в получены с использованием оценок соответственно [3, с. 104] и [4, с. 408].

Следствие 1. Если выполнены условия п. 3а теоремы, то

$$\exp(H^\delta + H^\tau) \leq \lambda_1 \lambda_r - \lambda_1 - \lambda_r + n(r + 1) - \sum_{i=1}^r \lambda_i.$$

Следствие вытекает из оценки числа Фробениуса [5, теорема 3.1.1] $g(\lambda_1, \dots, \lambda_r) \leq \lambda_1 \lambda_r - \lambda_1 - \lambda_r$, $r > 1$.

Данные оценки могут быть уточнены для частных классов перемешивающих матриц H базового преобразования генератора (δ, τ) -самоусечения.

ЛИТЕРАТУРА

1. Rueppel R. A. When shift registers clock themselves // Advances in Cryptology — Eurocrypt'87. LNCS. 1988. V. 304. P. 53–64.
2. Фомичев В. М. Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
3. Фомичев В. М. Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
4. Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. М.: ТВП, 2000. 448 с.
5. Alfonsin J. R. The Diophantine Frobenius Problem. Oxford University Press, 2005.

УДК 519.113.6

SIVCiphers — СИММЕТРИЧНЫЕ ИТЕРАТИВНЫЕ БЛОЧНЫЕ ШИФРЫ ИЗ БУЛЕВЫХ ФУНКЦИЙ С КЛЮЧЕВЫМИ АРГУМЕНТАМИ

Г. П. Агибалов

Вводится в рассмотрение класс SIVCipher много раундовых симметричных блочных шифров, в которых каждый раунд представлен инъективной системой булевых функций, зависящих существенно от ограниченного числа аргументов из информационного блока на входе раунда, и в которых раундовый ключ является подмножеством этих функций и (или) наборов их существенных аргументов. Современные симметричные блочные шифры с аддитивным раундовым ключом принадлежат этому классу. Описываются два других семейства шифров в классе SIVCipher — Фейстеля и Люцифер, построенных по известным одноимённым криптографическим схемам.

Ключевые слова: криптография, булевы функции, симметричные итеративные блочные шифры, сеть Фейстеля, шифр Люцифер.