Пример 2. Рассмотрим таблицы зашифрования эндоморфных шифров при $\lambda = \mu = 4$ с произвольными вероятностями ключей (табл. 3 и 4).

Таблица 3

№	K	x_1	x_2	x_3	x_4
1	k_1	1	4	3	2
2	k_2	1	3	2	4
3	k_3	2	1	3	4
4	k_4	3	2	4	1
5	k_5	4	2	1	3

Таблица 4

№	K	x_1	x_2	x_3	x_4
1	k_1	4	1	2	3
2	k_2	3	4	1	2
3	k_3	2	3	4	1
4	k_4	1	2	4	3
5	k_5	4	1	3	2
6	k_6	2	3	1	4

Это минимальные (по включению) транзитивные шифры, которые не могут быть совершенными ни при каких распределениях вероятностей ключей, причём из их таблиц зашифрования невозможно извлечь латинский квадрат.

Таким образом, в работе рассмотрена задача обобщения теоремы Шеннона для эндоморфных совершенных шифров. Построены примеры, показывающие, что минимальность шифра по числу ключей и минимальность по включению приводят к разным постановкам задач.

ЛИТЕРАТУРА

1. *Шеннон К.* Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001.
3. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003.
4. *Медведева Н. В., Титов С. С.* О неминимальных совершенных шифрах // Прикладная дискретная математика. Приложение. 2013. № 6. С. 42–44.
5. *Медведева Н. В., Титов С. С.* Неэндоморфные совершенные шифры с двумя шифрвеличинами // Прикладная дискретная математика. Приложение. 2015. № 8. С. 63–66.
6. *Медведева Н. В., Титов С. С.* Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. № 4 (30). С. 43–55.

УДК 519.1 DOI 10.17223/2226308X/9/26

О СПОСОБАХ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ ГЕНЕРАТОРОВ С ЗАДАННЫМ ПОКАЗАТЕЛЕМ БЕСПОВТОРНОСТИ ВЫХОДНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Д. А. Романько, В. М. Фомичев

В связи с понятием слабого ключа итеративного симметричного блочного шифра исследованы некоторые способы построения ключевого расписания, обеспечивающего отсутствие повторений в последовательности раундовых ключей. На основе генератора «1-2 шага», использующего линейные регистры сдвига длины n и m с максимальной длиной периода, построен автономный автомат с выходным алфавитом V_m, у которого при любом начальном состоянии отрезок длины 2^{m-1} выходной последовательности не содержит повторяющихся векторов.

Ключевые слова: *блочный шифр, раундовый ключ, r-бесповторная последовательность, r-бесповторный автомат, показатель бесповторности.*

Введение

При криптографическом анализе DES-алгоритма введено понятие слабого ключа, т. е. основного ключа, порождающего 16 одинаковых раундовых ключей. В [1, с. 298] для r-раундового блочного алгоритма использовано понятие μ-слабого ключа, порождающего ровно μ различных раундовых ключей, $1 \leqslant \mu < r$. Показано, что при определённых условиях использование слабых ключей ослабляет криптографические свойства итеративного блочного шифра. Поэтому представляет интерес задача построения ключевого расписания, генерирующего при любом основном ключе r различных раундовых ключей. Для решения применим теоретико-автоматный подход.

Основные обозначения:

— V_n — множество двоичных n-мерных векторов, $n \in \mathbb{N}$;
— $V_{n,0}$ — множество ненулевых двоичных n-мерных векторов, $n \in \mathbb{N}$;
— ЛРСmax-n — линейный регистр левого сдвига длины n максимального периода, $n \in \mathbb{N}$.

1. Бесповторность последовательностей и автономных автоматов

Пусть $X_{\to} = \{x_0, x_1, \ldots\}$ — конечная или бесконечная последовательность над X и $|X| = k$.

В последовательности $X_{\to}$ i-й r-граммой называется слово $(x_i, x_{i+1}, \ldots, x_{i+r-1})$ длины r в алфавите X, $i = 0, 1, 2, \ldots$; r-грамму назовём бесповторной, если она не содержит одинаковых символов. Последовательность r-грамм последовательности $X_{\to}$ обозначим $X^r_{\to}$.

Последовательность назовём r-бесповторной, если все её r-граммы бесповторные. Чисто периодическая последовательность $X_{\to}$ с длиной периода t является r-бесповторной, если бесповторными являются её i-е r-граммы при $i = 0, \ldots, t-1$.

Показателем бесповторности $X_{\to}$ (обозначение $\operatorname{urp} X_{\to}$) назовём наибольшее натуральное r, при котором последовательность $X_{\to}$ является r-бесповторной. Очевидно, $\operatorname{urp} X_{\to} \leqslant k$, и если последовательность $X_{\to}$ r-бесповторная, то она и r'-бесповторная при любом $r' \leqslant r$.

Автономный автомат $A = (S, Y, h, f)$, где S — множество состояний, Y — выходной алфавит, h — функция переходов, f — функция выходов, называется r-бесповторным, если при любом начальном состоянии A генерирует бесповторное выходное слово длины r. Показатель бесповторности инициального автомата A_s определим как показатель бесповторности выходной последовательности при начальном состоянии $s \in S$ и обозначим $\operatorname{urp} A_s$. Показателем бесповторности автомата A назовём $\operatorname{urp} A = \min\limits_{s \in S}\{\operatorname{urp} A_s\}$.

2. Примеры r-бесповторных автономных автоматов $A = (S, Y, h, f)$

1. Пусть $S = V_{n,0}$, $Y = V_r$, h — подстановка двоичного линейного регистра левого сдвига с примитивным характеристическим многочленом, $f(y_1, \ldots, y_n) = (y_1, \ldots, y_r)$, $r \geqslant n$. Автомат генерирует r-граммы линейной рекуррентной последовательности $X_{\to}$ (порядка n) максимального периода. Следовательно, $\operatorname{urp} X^r_{\to} = 2^n - 1$ при $r \geqslant n$.

2. Пусть $S = V_n$, $Y = V_r$, h — полноцикловая подстановка двоичного нелинейного регистра сдвига длины n, $f(y_1, \ldots, y_n) = (y_1, \ldots, y_r)$, $r \geqslant n$. Автомат генерирует r-граммы нормальной рекуррентной последовательности (де Брейна). Отсюда $\operatorname{urp} X^r_{\to} = 2^n$ при $r \geqslant n$.

Для построения ключевого расписания r-раундового блочного шифра без слабых ключей представляет интерес построение r-бесповторного автомата, где $\lambda > l \geqslant r$, $r \leqslant 32$ (здесь λ — длина основного бинарного ключа, l — длина раундовых бинарных ключей). Для построения такого автомата рассмотрим криптографический генератор «1-2 шага».

3. Криптографический генератор «1-2 шага»

Рассмотрим автономный автомат $A = (V_{n,0} \times V_{m,0}, V_{m,0}, h, \psi)$ с множеством состояний $V_{n,0} \times V_{m,0}$, выходным алфавитом $V_{m,0}$, функцией переходов h и функцией выходов ψ. При состоянии автомата $s = (y_1, \ldots, y_n, x_1, \ldots, x_m)$ выполнено $\psi(s) = (x_1, \ldots, x_m)$ и $h(s) = (\delta(y_1, \ldots, y_n), g^{a+1}(x_1, \ldots, x_m))$, где δ и g суть подстановки, реализуемые ЛРСmax-n и ЛРСmax-m соответственно, $a = f(y_1, \ldots, y_n)$, f — равновероятная булева функция, в простейшем случае $f(y_1, \ldots, y_n) = y_n$. Таким образом, «продвижение» генерирующего ЛРСmax-m в состоянии s равно $a + 1$, то есть 1 или 2 в зависимости от знака a, выработанного управляющим ЛРСmax-n. После $2^n - 1$ тактов «продвижение» генерирующего ЛРСmax-m равно $\tau = 2^n + 2^{n-1} - 1 - f(0, \ldots, 0)$ при любом начальном состоянии $s \in V_{n,0} \times V_{m,0}$.

Обозначим: $X_{\rightarrow}(s)$ — выходная последовательность автомата A при начальном состоянии s; $X_{\rightarrow}(s, t)$ — подпоследовательность последовательности $X_{\rightarrow}(s)$, составленная из первых t символов. Известно [1, с. 317], что длина периода последовательности $X_{\rightarrow}(s)$ равна $t = (2^n - 1)(2^m - 1)/\sigma$ при любом начальном состоянии s, где $\sigma = (\tau, 2^m - 1)$.

Теорема 1. При любом начальном состоянии s последовательность $X_{\rightarrow}(s, 2^{m-1})$ автомата A является бесповторной.

Справедливость теоремы следует из того, что $X_{\rightarrow}(s, 2^{m-1})$ есть бесповторная выборка (размера 2^{m-1}) с переменным шагом $1 - 2$ из периодического отрезка последовательности состояний ЛРСmax-m.

Отметим, что на основе автомата A можно построить ключевое расписание, удовлетворяющее указанным требованиям. Для этого следует положить: состояние s — основной ключ, длина основного бинарного ключа $\lambda = m + n$, длина раундовых бинарных ключей $l = m$, где $m > 5$. Тогда при любом числе раундов $r \leqslant 32$ выполнено условие бесповторности последовательности раундовых бинарных ключей. В частности, параметры ключевого расписания алгоритма DES достигаются при $m = 48$, $n = 8$, а параметры ключевого расписания алгоритма ГОСТ 28147-89 — при $m = 32$, $n = 224$.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.