ЛИТЕРАТУРА

1. *Rukhin A., Soto J., Nechvatal J., et al.* A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology, 2010.
2. *Barker E. and Kelsey D.* Recommendation for Random Bit Generator (RBG) Constructions (DRAFT NIST Special Publication 800-90C). National Institute of Standards and Technology, 2012.
3. *Рябко Б. Я., Фионов А. Н., Шокин Ю. И.* Криптография и стеганография в информационных технологиях. Новосибирск: Наука, 2015.
4. *Cover T. M. and Thomas J. A.* Elements of Information Theory. N.Y., USA: Wiley-Interscience, 2006.

УДК 519.1 DOI 10.17223/2226308X/9/28

О КЛЮЧЕВОМ РАСПИСАНИИ БЛОЧНЫХ ШИФРОВ БЕЗ СЛАБЫХ КЛЮЧЕЙ

В. М. Фомичев

Исследовано ключевое расписание симметричного r-раундового блочного шифра, при котором все раундовые ключи различны. Ключевое расписание реализуется как последовательное соединение автоматов: автономного автомата A, генерирующего выходную последовательность бинарных векторов с длиной периода не меньше r, и внутренне автономного автомата с постоянной памятью, в которой записан основной ключ блочного шифра. Рассмотрен пример, использующий в качестве автомата A линейный регистр сдвига с максимальной длиной периода.

Ключевые слова: *блочный шифр, раундовый ключ, бесповторная последовательность, показатель бесповторности последовательности.*

Введение

Используем следующие обозначения:

V_n — множество двоичных n-мерных векторов, $n \in \mathbb{N}$;

$X_{\rightarrow} = \{x_0, x_1, \ldots\}$ — последовательность над множеством X;

$\Gamma(A)$ — граф автомата Мили A;

$\langle H \rangle$ — линейная оболочка множества векторов H.

Свойства ключевого расписания, характеризующие взаимосвязи основного ключа с раундовыми ключами, являются определяющими при оценке стойкости итеративного блочного шифра (ИБШ) относительно ряда методов криптоанализа: согласования, дифференциального и др. Например, нежелательно ключевое расписание, при котором генерируемая из основного ключа последовательность раундовых ключей содержит определённое число повторяющихся элементов. Так, по отношению к основному ключу при криптографическом анализе DES-алгоритма введено понятие слабого ключа, то есть основного ключа, порождающего 16 одинаковых раундовых ключей. В [1, с. 298] для r-раундового блочного алгоритма это понятие обобщено до μ-слабого ключа, порождающего в наборе раундовых ключей $q_1, \ldots, q_r$ ровно μ различных элементов, $1 \leqslant \mu < r$. Показано, что при определённых условиях использование слабых ключей может привести к негативным последствиям с точки зрения обеспечения конфиденциальности данных. Криптографические свойства ИБШ считаются хорошими, если шифрующие подстановки близки по свойствам к случайным подстановкам, в частности, когда набор раундовых ключей $q_1, \ldots, q_r$ есть случайная бесповторная выборка из множества двоичных векторов заданной размерности. В связи с этим возникает задача построения ключевого расписания, исключающего возможность повторений раундовых ключей в генерируемом наборе.

1. Постановка задачи

Рассмотрим ключевое расписание θ для итеративного r-раундового блочного алгоритма, $n, m, r \in \mathbb{N}$. Функция $\theta : V_n \to V_{mr}$ отображает основной n-битовый ключ $k = (k_1, \ldots, k_n)$ в набор m-битовых раундовых ключей $q_1, \ldots, q_r$. Функцию θ зададим системой координатных функций $\{\theta_1, \ldots, \theta_r\}$, где $\theta_i : V_n \to V_m$ отображает основной n-битовый ключ в раундовый ключ q_i, $i = 1, \ldots, r$. Обычно выполнены соотношения $m < n < mr$, при этих соотношениях функция θ не сюръективная и, следовательно, система функций $\{\theta_1, \ldots, \theta_r\}$ алгебраически зависимая.

Требуется построить функцию θ со свойством: при любом ключе $(k_1, \ldots, k_n) \in V_n$ набор $\theta_1(k_1, \ldots, k_n), \ldots, \theta_r(k_1, \ldots, k_n)$ состоит из r различных m-мерных векторов. Такую функцию θ назовем ключевым расписанием без слабых ключей. В [2] такая функция построена на основе генератора «1-2 шага».

2. Бесповторность последовательностей и автономных автоматов

Последовательности $X_{\to} = \{x_0, x_1, \ldots\}$ над конечным множеством X однозначно соответствует последовательность r-грамм $X^r_{\to} = \{(x_i, x_{i+1}, \ldots, x_{i+r-1})\}$, где $i = 0, 1, \ldots, l-r$ для конечной последовательности $X_{\to}$ длины $l > r$ и $i = 0, 1, 2, \ldots$, если $X_{\to}$ бесконечная. Назовём r-грамму $(x_0, x_1, \ldots, x_{r-1})$ *бесповторной*, если $x_i \neq x_j$ при $i \neq j$, $i, j \in 0, 1, \ldots, r-1$. Последовательность $X_{\to}$ назовём *r-бесповторной*, если последовательность $X^r_{\to}$ состоит из бесповторных r-грамм (тогда $X_{\to}$ является ρ-бесповторной, где $1 \leqslant \rho \leqslant r$). *Показателем бесповторности* $X_{\to}$ (обозначается $\mathrm{urp}X_{\to}$) назовём наибольшее r, при котором $X_{\to}$ является r-бесповторной.

Из определений следует, что периодическая последовательность $X_{\to}$ с длиной периода t является r-бесповторной, если бесповторными являются r-граммы $(x_i, x_{i+1}, \ldots, x_{i+r-1})$, $i = 0, 1, \ldots, t-1$.

Пусть $A = (S, Y, h, f)$ — перестановочный автономный автомат, где S, Y — соответственно внутренний и выходной алфавиты; $h : S \to S$ — биективная функция переходов; $f : S \to Y$ — функция выходов. Известно, что автомат A при начальном состоянии s_0, проходя периодическую последовательность состояний $\{s_0, s_1, \ldots, s_{\tau-1}\}$ с длиной периода τ, генерирует периодическую выходную последовательность $\{y_0, y_1, \ldots, y_{\tau-1}\}$ с длиной периода t, где t делит τ, $y_i = f(s_i)$, $i = 0, 1, \ldots$

Рассмотрим слабо инициальный автомат [1, с. 148] $(A, W) = ((S, W), Y, h, f)$, $\varnothing \neq W \subseteq S$, где W — множество допустимых начальных состояний автомата. В частности, при фиксированном начальном состоянии $s \in S$ имеем инициальный автомат (обозначаемый A_s).

Автомат A (автомат (A, W)) называется *r-бесповторным*, если r-бесповторной является выходная последовательность автомата при любом начальном состоянии $s \in S$ ($s \in W$). *Показателем бесповторности* автомата A (автомата (A, W), инициального автомата A_s) назовём наибольшее натуральное r, такое, что выходная последовательность автомата A является r-бесповторной при любом начальном состоянии $s \in S$ (при любом $s \in W$, при фиксированном $s \in S$). Обозначим показатели бесповторности автоматов A, (A, W) и A_s соответственно через $\mathrm{urp}A$, $\mathrm{urp}(A, W)$ и $\mathrm{urp}A_s$.

Утверждение 1.

а) $\mathrm{urp}A = \min\limits_{s\in S}\{\mathrm{urp}A_s\}$, $\mathrm{urp}(A,W) = \min\limits_{s\in W}\{\mathrm{urp}A_s\}$;

б) $\mathrm{urp}A_s$ не превышает длины периода выходной последовательности автомата A_s;

в) если состояния s и z принадлежат общему циклу графа автомата A, то $\mathrm{urp}A_s = \mathrm{urp}A_z$.

3. Схема ключевого расписания без слабых ключей

Пусть $p,m,u \in \mathbb{N}$, где $1 < p \leqslant u \leqslant r$. Обозначим $A = (V_p, V_u, h, f)$ — автономный автомат, где V_p — внутренний алфавит, V_u — выходной алфавит, $h : V_p \to V_p$ — функция переходов, $f : V_p \to V_u$ — функция выходов; $G = (V_u, V_{um}, V_m, \phi)$ — автомат с постоянной памятью [1, с. 148], т. е. внутренне автономный автомат с тождественной функцией переходов, где V_u — входной алфавит, V_{um} — внутренний алфавит, V_m — выходной алфавит. Определим функцию выходов $\phi : V_u \times V u_m \to V_m$ — если в памяти автомата G записана система векторов $k^{(1)},\ldots,k^{(u)}$ из V_m, то $\phi(\alpha, k^{(1)},\ldots,k^{(u)}) = \alpha_1 k^{(1)} \oplus \ldots \oplus \alpha_u k^{(u)}$ при входном символе $\alpha = (\alpha_1,\ldots,\alpha_u) \in V_u$.

Рассмотрим последовательное соединение управляющего автономного автомата A и генерирующего автомата G, обозначаемое $A \to G$. Представим n-битовый секретный ключ k в виде набора m-битовых подключей: $k = (k^{(1)},\ldots,k^{(u)})$.

Теорема 1. Если автомат A_s генерирует t-бесповторную периодическую последовательность с длиной периода t и в памяти автомата G записана линейно независимая система векторов $k^{(1)},\ldots,k^{(u)}$, то автомат $(A \to G)_z$ генерирует при $z = (s, k^{(1)},\ldots,k^{(u)})$ t-бесповторную периодическую последовательность с длиной периода t и $\mathrm{urp}(A \to G)_z = t$.

Доказательство. Выходная последовательность автомата $A \to G$ состоит из элементов линейной оболочки $\langle k^{(1)},\ldots,k^{(u)}\rangle$. Если $\alpha,\beta \in V_u$ и $\alpha \neq \beta$, то $\phi(\alpha, k^{(1)}, \ldots, k^{(u)}) \neq \phi(\beta, k^{(1)},\ldots,k^{(u)})$ в силу линейной независимости системы векторов $k^{(1)},\ldots,k^{(u)}$. Тогда в силу t-бесповторности выходной последовательности автомата A_s последовательность $\{\phi(\alpha_i, k^{(1)},\ldots,k^{(u)}) : i = 0,1,\ldots,t-1\}$ состоит из различных векторов, то есть автомат $(A \to G)_z$ является t-бесповторным. Вместе с тем $\phi(\alpha_i, k^{(1)},\ldots,k^{(u)}) = \phi(\alpha_{i+t}, k^{(1)},\ldots,k^{(u)})$, $i = 0,1,\ldots$, значит, $\mathrm{urp}(A \to G)_z = t$. ∎

4. Выбор параметров ключевого расписания без слабых ключей

Рассмотрим данную схему в качестве альтернативы ключевому расписанию блочного шифра ГОСТ 28147-89. Параметры в этом случае принимают значения $p = u = 8$, $m = 32$. Автомат A построим на основе линейного регистра сдвига длины 8 с примитивным характеристическим многочленом, выходными символами являются 8-граммы (байты) линейной рекуррентной последовательности. Следовательно, автомат A генерирует 255-бесповторную последовательность байтов. В соответствии с теоремой 1 автомат $(A \to G)_z$ при любом ненулевом состоянии s автомата A и линейно независимой системе векторов $k^{(1)},\ldots,k^{(8)}$ генерирует 255-бесповторную периодическую последовательность 32-битовых векторов с длиной периода 255 и $\mathrm{urp}(A \to G)_z = 255$.

Для ключевого расписания без слабых ключей 32-раундового блочного шифра достаточно взять любую бесповторную выборку размера 32 из выходной последовательности автомата $(A \to G)_z$, полученную при любом ненулевом состоянии s автомата A.

Ограничение на секретный ключ, связанное с линейной независимостью векторов, не является сильным. Если векторы $k^{(1)},\ldots,k^{(8)}$ выбраны случайно равновероятно из V_{32}, то вероятность линейной независимости системы равна $\prod\limits_{i=0}^{7}(1-2^{i-32})$, то есть превышает $1-2^{24}$.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
2. *Романько Д. А., Фомичев В. М.* О способах построения криптографических генераторов с заданным показателем бесповторности выходных последовательностей // Прикладная дискретная математика. Приложение. 2016. № 9. С. 65–67.

УДК 004.056.55 DOI 10.17223/2226308X/9/29

КРИПТОАНАЛИЗ КРИПТОСИСТЕМЫ МАК-ЭЛИСА, ПОСТРОЕННОЙ НА $(k-1)$-ПОДКОДАХ КОДА РИДА — МАЛЛЕРА

И. В. Чижов, М. А. Бородин

Описаны два вида криптосистем Мак-Элиса, построенных на подкодах кода Рида — Маллера. Изучен вопрос эквивалентных ключей для этих криптосистем. Получен результат о сводимости одной криптосистемы к другой. Приведены алгоритмы, которые позволяют применить атаку Чижова — Бородина к рассматриваемым криптосистемам для некоторых параметров кодов Рида — Маллера.

Ключевые слова: *криптосистема Мак-Элиса, подкоды Рида — Маллера, автоморфизмы кодов Рида — Маллера, произведение Шура, квадрат кода.*

Криптосистема Мак-Элиса предложена в 1978 г. Р. Дж. Мак-Элисом. Её стойкость основана на предположении сложности декодирования кода общего положения. Оригинальная криптосистема Мак-Элиса строится на двоичных кодах Гоппы. Для повышения эксплуатационных характеристик В. М. Сидельников предложил использовать коды Рида — Маллера [1]. Однако в 2007 г. Л. Миндера и А. Шокроллахи предложили достаточно эффективную атаку на такую криптосистему [2]. Кроме того, в 2013 г. Бородин и Чижов ещё больше понизили стойкость этой криптосистемы, а также построили полиномиальную атаку в случае использования кода Рида — Маллера $RM(r,m)$ с такими параметрами, что $(r,m-1)=1$ [3].

Бывает, что атаки на кодовые криптосистемы, работающие в случае использования полного кода, оказываются бесполезными в случае использования некоторых подкодов кода. Так была предложена криптосистема Бергера — Луадро, построенная на подкодах кода Рида — Соломона. В работе рассматриваются два аналога криптосистемы Бергера — Луадро, построенных на $(k-1)$-подкодах кода Рида — Маллера $RM(r,m)$.

Пусть V_n — множество всех двоичных векторов длины n. Известно, что с каждой булевой функцией $f(x_1,x_2,\ldots,x_m) : V_m \to V_1$ можно связать вектор значений $\Omega_f=(f(0,0,\ldots,0),f(0,0,\ldots,1),\ldots,f(1,1,\ldots,1))$. В дальнейшем не будем делать различий в обозначениях между булевой функцией и её вектором значений. Каждая булева функция может быть представлена полиномом Жегалкина: $f(x_1,x_2,\ldots,x_m) = \bigoplus\limits_{u=(u_1,u_2,\ldots,u_m)\in V_m} g_f(u)x^u$, здесь $x^u=x_1^{u_1}x_2^{u_2}\ldots x_m^{u_m}$ и $x_i^{u_i}=x_i$, если $u_i=1$, и $x_i^{u_i}=1$, если $u_i=0$, а $g_f(u)$ — некоторая булева функция.

Определение 1. Степенью булевой функции называется наименьшее целое положительное число d, такое, что $g_f(u)=0$ для всех u веса больше d, т. е. $\mathrm{wt}(u)>d$.