Теорема 1. Пусть g — произвольная подстановка из $S(\mathbb{Z}_n)$ и подмножество $W_1 \subseteq \subseteq ED_g$ таково, что $|W_1| = \lceil n/2 \rceil$, $0 \notin W_1$. Тогда для каждого $\alpha \in W_1$ выполняется равенство $\hat{p}_{\alpha,W_2}(g) = \hat{p}_{\alpha',W_1}(g)$, где $\alpha' = n - \alpha$ и

$$W_2 = \begin{cases} \{n-\alpha : \alpha \in W_1\}, & \text{если } n \text{ нечётно,} \\ \{n-\alpha : \alpha \in W_1\} \backslash \{n/2\}, & \text{если } n \text{ чётно.} \end{cases}$$

ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* $\otimes_{\mathbf{W},\mathrm{ch}}$-марковские преобразования // Прикладная дискретная математика. Приложение. 2015. Вып. 8. С. 17–19.
2. *Кемени Д., Снелл Д.* Конечные цепи Маркова. М.: Наука, 1970.

УДК 519.1 DOI 10.17223/2226308X/10/38

О МАТЕМАТИЧЕСКИХ МОДЕЛЯХ ПЕРЕМЕШИВАНИЯ КЛЮЧА В ИТЕРАТИВНЫХ БЛОЧНЫХ АЛГОРИТМАХ ШИФРОВАНИЯ[1]

Д. А. Романько, В. М. Фомичев

Представлена математическая модель перемешивания алгоритмами блочного шифрования битов ключа $k \in \{0,1\}^l$. Для симметричного итеративного r-раундового блочного алгоритма шифрования пусть B_q — множество номеров координат ключевого вектора k, от которых существенно зависит раундовый ключ q; q_i — λ-битовый ключ i-го раунда; ϕ_{q_i} — подстановка i-го раунда; A — матрица существенной зависимости раундовой функции ϕ; $\Phi_p = \phi_{q_p} \cdot \ldots \cdot \phi_{q_1}$, $i, p \in \{1, \ldots, r\}$; ρ — наименьшее натуральное число, при котором каждый бит ключа k является существенной переменной функции Φ_p, $\rho \in \{1, \ldots, r\}$. Для блочного алгоритма показателем $p(q_i)$ относительно раундового ключа q_i (ключевым показателем $p(k)$) называется наименьшее натуральное число $p \in \{1, \ldots, r\}$, при котором каждый бит блока данных $\Phi_p(x)$ существенно зависит от каждого бита раундового ключа q_i (ключа k).

Если $B_{q_i} \cap B_{q_j} = \varnothing$ для всех $i, j \in \{1, \ldots, \rho\}$, $i \neq j$, h и h' — подстановки множества $\{0,1\}^\lambda$, то: 1) если выходной блок алгоритма зависит от каждого бита ключа k, то $p(k) = p(q_1) + (\rho - 1)$; $p(q_i) = p(q_1) + (i-1)$ для $i = 1, \ldots, \rho$; 2) $p(k) \geqslant \geqslant I*\text{-exp}\, A + (\rho - 1)$, где $I = \{1, \ldots, n\}$, если $\phi(x, q) = h(x \oplus q)$, и $I = \{1\}$, если $\phi(x, q) = h'((x + q) \bmod 2^\lambda)$; здесь $I*\text{-exp}\, A$ — локальный экспонент матрицы A. Дана оценка ключевого показателя для итеративных блочных шифров Фейстеля, в частности $p(k) \geqslant 10$ для ГОСТ 28147-89.

Ключевые слова: *итеративный блочный алгоритм, локальный экспонент, ключевой показатель итеративного блочного алгоритма.*

Введение

К необходимым условиям обеспечения высокой стойкости блочного шифрования относится зависимость каждого бита выходного блока от всех битов входного блока и ключа (полное перемешивание), что достигается с помощью конструирования сложных функциональных связей между входными и выходными данными алгоритма с использованием итеративного принципа и свойств ключевого расписания.

Перемешивание битов входных данных оценивается обычно с помощью определения экспонентов перемешивающих орграфов раундовых подстановок. Обзор результа-

[1]Работа второго автора выполнена в соответствии с грантом РФФИ № 16-01-00226.

тов по оцениванию экспонентов различных классов матриц и орграфов можно найти в [1, гл. 11].

Перемешивание битов ключа имеет особенности, связанные с тем, что ключевые биты вводятся в алгоритм шифрования в ходе нескольких раундов и не всегда регулярным образом. В связи с этим исследование перемешивания блочным алгоритмом ключевых битов требует существенного развития математической модели по сравнению с моделью перемешивания входных блоков. Работа посвящена описанию данных моделей и получению оценок характеристик перемешивания битов ключа через локальные экспоненты перемешивающего орграфа раундовой подстановки.

1. Определяющие свойства ключевого перемешивания блочного алгоритма

Пусть $\mathcal{A}$ есть блочный r-раундовый алгоритм шифрования, где блок данных $x \in \in V_n = \{0,1\}^n$.

Обозначим: $K = V_l$ — ключевое множество алгоритма; V_λ — область значений раундовых ключей; $\phi(x,q) : V_n \times V_\lambda \to V_n$ — биективная по переменной x раундовая функция; ϕ_q — раундовая подстановка, полученная из $\phi(x,q)$ при фиксации раундового ключа значением q; q_i — раундовый i-й ключ, генерируемый при основном ключе k алгоритма, $i = 1,\dots,r$; g_k — шифрующая подстановка алгоритма $\mathcal{A}$, реализуемая при ключе $k \in K$.

В данных обозначениях λ, l — длины соответственно раундовых ключей и ключа итеративного блочного алгоритма; уравнение шифрования имеет вид $y = g_k(x)$, где шифрующая подстановка определена равенством $g_k = \phi_{q_r} \cdot \ldots \cdot \phi_{q_1}$.

Обозначим B_q множество всех номеров координат ключевого вектора k, от которых существенно зависит раундовый ключ q; тогда выполнено покрытие

$$\{1,\dots,l\} = B_{q_1} \cup \ldots \cup B_{q_r}. \tag{1}$$

В зависимости от свойств ключевого расписания (зависимы или независимы раундовые ключи) для блоков покрытия (1) множества $\{1,\dots,l\}$ возможны варианты:

$$B_{q_i} \cap B_{q_j} = \varnothing \text{ для всех } i,j \in \{1,\dots,r\},\ i \neq j;$$
$$B_{q_i} \cap B_{q_j} \neq \varnothing \text{ при некоторых } i,j \in \{1,\dots,r\}.$$

Обозначим Φ_p композицию раундовых подстановок $\Phi_p = \phi_{q_p} \cdot \ldots \cdot \phi_{q_1}, p = 1,\dots,r$.

Показателем алгоритма $\mathcal{A}$ относительно раундового ключа q_i называется наименьшее натуральное число $p \in \{1,\dots,r\}$ (если такое число существует), при котором каждый бит блока данных $\Phi_p(x)$ существенно зависит от каждого бита раундового ключа q_i, обозначим эту величину $p(q_i)$, $i = 1,\dots,r$. По определению $p(q_i) \geqslant i$.

Ключевым показателем алгоритма $\mathcal{A}$ называется наименьшее натуральное число $p \in \{1,\dots,r\}$ (если такое число существует), при котором каждый бит блока данных $\Phi_p(x)$ существенно зависит от каждого бита ключа k, обозначим эту величину $p(k)$.

Из определения следует, что если показатель $p(k)$ алгоритма $\mathcal{A}$ существует, то $\min\limits_{1\leqslant i\leqslant r} p(q_i) \leqslant p(k) \leqslant r$. Установим более точно связь между введёнными ключевыми показателями.

2. Оценка ключевого показателя итеративного блочного алгоритма

Определим $\rho(\mathcal{A})$ (кратко ρ) как наименьшее натуральное число $p \in \{1,\dots,r\}$ (если такое число существует), при котором каждый бит ключа k является существенной

переменной хотя бы для одной из раундовых функций $\phi_{q_1}, \ldots, \phi_{q_p}$. Это определение позволяет уточнить разбиение (1):

$$\{1, \ldots, l\} = B_{q_1} \cup \ldots \cup B_{q_\rho}. \tag{2}$$

Теорема 1. Если выходной блок алгоритма $\mathcal{A}$ зависит от каждого бита ключа k и $B_{q_i} \cap B_{q_j} = \varnothing$ для всех $i, j \in \{1, \ldots, \rho\}$, $i \neq j$, то

$$p(q_i) = p(q_1) + (i-1), \quad i = 1, \ldots, \rho,$$
$$p(k) = p(q_1) + (\rho - 1).$$

Обозначим: ϕ_q^j — j-я координатная функция раундовой функции ϕ_q, $j = 1, \ldots, n$; $A = (a_{i,j})$ — перемешивающая матрица порядка n (матрица существенной зависимости) раундовой функции ϕ_q, где $a_{i,j} = 1$ тогда и только тогда, когда ϕ_q^j зависит существенно от x_i; в противном случае $a_{i,j} = 0$.

Пусть $\varnothing \neq I \subseteq \{1, \ldots, n\}$ и матрица $A(I*)$ размера $s \times n$ получена из A вычёркиванием строк с номерами $i \notin I$. Наименьшее натуральное число γ, такое, что матрица $A^t(I*)$ состоит из положительных чисел для любого $t \geqslant \gamma$, называется $I*$-экспонентом матрицы A [2], обозначается $I*\text{-}\exp A$ (кратко γ_{I*}).

Показатели $p(q_i)$ и $p(k)$ алгоритма $\mathcal{A}$ зависят не только от свойств покрытий (1) и (2), определяемых ключевым расписанием алгоритма, но и от способа подмешивания ключа и других свойств алгоритма.

Теорема 2. Если выполнено разбиение (2) и $B_{q_i} \cap B_{q_j} = \varnothing$ для всех $i, j \in \{1, \ldots, \rho\}$, $i \neq j$, то $p(k) \geqslant \gamma_{I*} + (\rho - 1)$, где

1) $I = \{1, \ldots, n\}$, если $\phi(x, q) = h(x \oplus q)$;
2) $I = \{1\}$, если $\phi(x, q) = h'((x + q) \bmod 2^\lambda)$.

Здесь $x, q \in V_\lambda$; h и h' — подстановки множества V_λ.

Пример. Итеративный блочный шифр Фейстеля.

При реализации раундовой функции Фейстеля n-битовый блок входных данных x разбивается на подблоки x' и x'' по $n/2$ бит, n чётное, то есть $\lambda = n/2$. Раундовая подстановка определена равенством $\phi(x, q) = (x'', x' \oplus \psi(x'', q))$, где $\psi(x'', q) : V_{n/2} \times \times V_{n/2} \to V_{n/2}$. Тогда по теореме 2 $p(k) \geqslant \gamma_{I*} + (\rho - 1)$, где

1) $I = \{n/2 + 1, n/2 + 2, \ldots, n\}$, если $\psi(x'', q) = h(x'' \oplus q)$;
2) $I = \{n/2 + 1\}$, если $\psi(x'', q) = h'((x'' + q) \bmod 2^\lambda)$.

В частности, для алгоритма ГОСТ 28147-89 (случай 2) следует положить $n = 64$, $\rho = 8$. Из теоремы 2 получаем $p(k) \geqslant \gamma_{I*} + 7$, где $I = \{33\}$. С помощью вычислительного эксперимента на ЭВМ для данного алгоритма посчитано $\gamma_{I*} = 3$, $\exp A = 5$.

В качестве рекомендации для разработчиков по результатам вычислений получены нижние оценки числа r раундов шифрования при использовании операции сложения по модулю 2^{32} для подмешивания раундовых ключей:

1) в условиях модели перемешивания битов входных данных $r \geqslant 5$;
2) в условиях модели перемешивания ключевых битов с использованием экспонента раундовой подстановки $r \geqslant 12$;
3) в условиях модели перемешивания ключевых битов с использованием локального экспонента раундовой подстановки $r \geqslant 10$.

Наиболее точной является оценка, полученная в условиях третьей модели.

Развитие математического аппарата для оценки перемешивания ключевой информации в итеративных блочных алгоритмах позволяет уточнить приемлемые границы для значений важных параметров блочных шифров.