УДК 519.7 DOI 10.17223/2226308X/10/37

О СВОЙСТВАХ W-ПОДСТАНОВОК НАД КОЛЬЦОМ ВЫЧЕТОВ

М. А. Пудовкина, А. С. Макеев

Известно, что состояния цепи Маркова можно укрупнить разбиением $\mathbf{W}$ множества $\mathbb{Z}_n$, если выполнен ряд условий на блоки разбиения и элементы матрицы разностей переходов подстановки $g \in S(\mathbb{Z}_n)$. Однако в модификации разностного метода криптоанализа данное требование можно смягчить и требовать его выполнения только для одного блока W разбиения $\mathbf{W}$. В связи с этим в работе рассматриваются подстановки, удовлетворяющие «смягчённому» требованию для блока W, названные W-подстановками, и описываются их свойства.

Ключевые слова: *марковские алгоритмы блочного шифрования, укрупнения цепей Маркова, W-подстановка, разностный метод.*

В настоящее время в большинстве итерационных алгоритмов блочного шифрования сложение с раундовым ключом осуществляется над n-мерным векторным пространством над полем GF(2) или над кольцом вычетов $\mathbb{Z}_{2^n}$. Примерами таких алгоритмов являются ГОСТ 28147-89, BelT и FEAL.

Одним из основных методов анализа алгоритмов блочного шифрования является разностный метод и его модификации. Необходимость формального описания ряда модификаций разностного метода накладывает дополнительные ограничения на свойства преобразований, являющихся компонентами раундовой функции. Одним из таких является условие $+_{\mathbf{W}}$-марковости s-боксов [1], а кроме того, условие $+_{\mathbf{W}}$-марковости раундовой функции. Однако на практике для многих алгоритмов блочного шифрования данные условие выявить «трудно». Поэтому вводятся понятия, смягчающие данные требования, которые «легче» применять на практике.

Пусть $\mathbb{N}$ — множество натуральных чисел; $\mathbb{Z}_n$ — кольцо вычетов по модулю $n \in \mathbb{N}$, $n \geqslant 2$; $S(\mathbb{Z}_n)$ — симметрическая группа на $\mathbb{Z}_n$; $\alpha^b = b(\alpha)$ — образ элемента $\alpha \in \mathbb{Z}_n$ при действии на него подстановкой $b \in S(\mathbb{Z}_n)$. Для произвольной подстановки $b \in S(\mathbb{Z}_n)$ положим

$$\hat{p}_{\theta,\varepsilon}(b) = 2^{-n}|\{\alpha \in \mathbb{Z}_n : (\theta+\alpha)^b = \varepsilon + \alpha^b\}|,\ \theta,\varepsilon \in \mathbb{Z}_n,$$
$$\hat{p}_{\theta,W}(b) = \sum_{\theta' \in W} \hat{p}_{\theta,\theta'}(b),\ \theta \in \mathbb{Z}_n, W \subseteq \mathbb{Z}_n.$$

Определение 1. Пусть $W \subseteq \mathbb{Z}_n$. Назовём $b \in S(\mathbb{Z}_n)$ W-подстановкой, если для любых элементов $\theta, \theta' \in W$ выполняется равенство $\hat{p}_{\theta,W}(b) = \hat{p}_{\theta',W}(b)$.

Для подстановки $g \in S(\mathbb{Z}_n)$ через ED_g обозначим множество, состоящее из всех таких подмножеств $W \subseteq \mathbb{Z}_n$, что для любого элемента $\alpha \in W$ существует элемент $\beta \in \mathbb{Z}_n$, удовлетворяющий условию $(\alpha+\beta)^g - \beta^g \in W$.

Доказано, что любая подстановка $g \in S(\mathbb{Z}_n)$ является W-подстановкой для некоторого подмножества $W \subseteq ED_g$. Отсюда следует оценка снизу мощности множества ED_g, а именно $|ED_g| \geqslant \lceil n/2 \rceil$.

Доказана замкнутость множества ED_g относительно операции объединения подмножеств. Так, если $g \in S(\mathbb{Z}_n)$, то для любых подмножеств $W, W' \subseteq ED_g$ выполняется включение $W \cup W' \subseteq ED_g$. Кроме того, показано существование ровно n таких подстановок $g \in S(\mathbb{Z}_n)$, что $|ED_g| = n(n-1)/2$.

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.