УДК 519.7 DOI 10.17223/2226308X/8/6

$\otimes_{\mathbf{W},\mathrm{ch}}$-МАРКОВСКИЕ ПРЕОБРАЗОВАНИЯ

Б. А. Погорелов, М. А. Пудовкина

Разностный криптоанализ итеративных алгоритмов блочного шифрования с алфавитом текстов X, как правило, проводится в рамках марковской модели. При этом фиксируется регулярная абелева группа $(X, \otimes)$ и используется тот факт, что для $\otimes$-марковских алгоритмов блочного шифрования последовательность разностей (относительно операции $\otimes$) пар промежуточных шифртекстов i-го раунда, $i = 1, 2, \ldots$, образует цепь Маркова. В работе рассматриваются $\otimes$-марковские алгоритмы блочного шифрования, у которых существует укрупнение состояний цепи Маркова до блоков разбиения $\mathbf{W}$, также являющееся цепью Маркова. Такие алгоритмы блочного шифрования, а также подстановки на X вместе с операцией $\otimes$ наложения ключа, задающие раундовую функцию алгоритма шифрования, названы $\otimes_{\mathbf{W},\mathrm{ch}}$-марковскими. Получены условия на блоки разбиения $\mathbf{W}$ и элементы матрицы разностей переходов раундовой функции, при которых алгоритм блочного шифрования является $\otimes_{\mathbf{W},\mathrm{ch}}$-марковским. Приведены преобразования, основанные на операциях экспоненцирования и логарифмирования в кольце вычетов $\mathbb{Z}_n$ и поле $\mathrm{GF}(n+1)$, а также указаны разбиения $\mathbf{W}$, при которых данные преобразования являются $+_{\mathbf{W},\mathrm{ch}}$-марковскими относительно соответствующей операции сложения $+$ в кольце или поле.

Ключевые слова: *марковский алгоритм блочного шифрования, цепи Маркова, метод усечённых разностей, экспоненциальные преобразования.*

Пусть $(X, \otimes)$ — произвольная регулярная абелева группа на конечном множестве X с бинарной операцией $\otimes$ и единичным элементом e; α^{-1} — обратный к α элемент относительно операции $\otimes$, $\alpha \otimes \beta^{-1} = \alpha \bar{\otimes} \beta$ для любых $\alpha, \beta \in X$; $X^{\times} = X \setminus \{e\}$; $S(X)$ — симметрическая группа на X; $\alpha^g = \alpha g = g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$; $K^{(i)}$ — множество всех раундовых ключей i-го раунда, $k^{(i)} \in K^{(i)}$; $g^{(i)} : (x, k^{(i)}) \mapsto g^{(i)}(x, k^{(i)})$ и $g^{(i)}_{k^{(i)}} : \alpha \mapsto g^{(i)}(\alpha, k^{(i)})$ — раундовые функция i-го раунда, где $x \in X$, $k^{(i)} \in K^{(i)}$; $f_{\mathbf{k}_t} = g^{(1)}_{k^{(1)}} \cdot \ldots \cdot g^{(t)}_{k^{(t)}}$ для $\mathbf{k}_t = (k^{(1)}, \ldots, k^{(t)}) \in K^{(1)} \times \ldots \times K^{(t)}$;

$$p_{\theta,\varepsilon}\left(g^{(i)}\right) = \left|\left\{(\alpha, k^{(i)}) \in X \times K^{(i)} : (\theta \otimes \alpha)^{g^{(i)}_{k^{(i)}}} = \varepsilon \otimes \alpha^{g^{(i)}_{k^{(i)}}}\right\}\right| \cdot \left|K^{(i)}\right|^{-1} \cdot |X|^{-1}.$$

В [1] показано, что если $\xi^{(0)}$ — дискретная случайная величина на множестве $X^{\times}$, то в l-раундовом $\otimes$-марковском алгоритме блочного шифрования с независимыми и равномерно распределёнными раундовыми ключами раундовые разности $\xi^{(t)} = \left(\xi^{(0)} \otimes \alpha\right)^{f_{\mathbf{k}_t}} \bar{\otimes} \alpha^{f_{\mathbf{k}_t}}$, являясь случайными величинами, образуют однородную цепь Маркова.

Для $\mathbf{W}$-разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ множества X рассмотрим последовательность таких дискретных случайных величин $\tilde{\xi}^{(0)}_{\mathbf{W}}, \ldots, \tilde{\xi}^{(l)}_{\mathbf{W}}$ на множестве $\{0, \ldots, r-1\}$, что $\tilde{\xi}^{(t)}_{\mathbf{W}} = j$ тогда и только тогда, когда $\xi^{(t)} \in W_j$, $j \in \{0, \ldots, r-1\}$, $t = 1, \ldots, l$. Для $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ и $i = 1, \ldots, l$ положим

$$p_{\theta,W_c}\left(g^{(i)}\right) = \sum_{\theta' \in W_c} p_{\theta,\theta'}\left(g^{(i)}\right), \theta \in X^{\times}.$$

Приведём условия, при которых для $\otimes$-марковского алгоритма блочного шифрования последовательность случайных величин $\tilde{\xi}^{(0)}_{\mathbf{W}}, \ldots, \tilde{\xi}^{(l)}_{\mathbf{W}}$ является цепью Маркова.

Утверждение 1. Пусть для итерационного l-раундового $\otimes$-марковского алгоритма блочного шифрования с раундовой функцией i-го раунда $g^{(i)}$ разбиение $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, $r \geqslant 2$, множества X ($X^{\times}$) таково, что:

1) $\mathbf{P}\left\{\xi^{(0)} = \theta^{(0)}\right\} = \mathbf{P}\left\{\xi^{(0)} = \theta'^{(0)}\right\}$ для всех $\theta^{(0)}, \theta'^{(0)} \in W_c$, $c \in \{0, \ldots, r-1\}$;
2) для каждых $(c, j) \in \{0, \ldots, r-1\}^2$, $(\theta, i) \in W_j \times \{1, \ldots, l\}$ и некотором $a_{j,c}^{(i)}$, $0 \leqslant a_{j,c}^{(i)} \leqslant 1$, выполняется равенство $p_{\theta, W_c}\left(g^{(i)}\right) = a_{j,c}^{(i)}$.

Тогда последовательность случайных величин $\tilde{\xi}_{\mathbf{W}}^{(0)}, \ldots, \tilde{\xi}_{\mathbf{W}}^{(l)}$ над $\{0, \ldots, r-1\}$ образует цепь Маркова. Если $g^{(1)} = g^{(2)} = \ldots = g^{(l)}$, то эта цепь Маркова является однородной.

Определение 1. Назовём l-раундовый $\otimes$-марковский алгоритм блочного шифрования $\otimes_{\mathbf{W},\mathrm{ch}}$-марковским для разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, $r \geqslant 2$, если последовательность случайных величин $\tilde{\xi}_{\mathbf{W}}^{(0)}, \ldots, \tilde{\xi}_{\mathbf{W}}^{(l)}$ является цепью Маркова, т. е. раундовая функция $g^{(i)}$ удовлетворяет п. 2 утверждения 1.

Определение 2. Назовём преобразование $b \in S(X)$ $\otimes_{\mathbf{W},\mathrm{ch}}$-марковским для разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, $r \geqslant 2$, если для каждых $(c, j) \in \{0, \ldots, r-1\}^2$, $\theta \in W_j$ и некоторых $a_{j,c}$, $0 \leqslant a_{j,c} \leqslant 1$, выполняется равенство $p_{\theta, W_c}(b) = a_{j,c}$.

Отметим, что неявно допущение о $\otimes_{\mathbf{W},\mathrm{ch}}$-марковости алгоритма блочного шифрования для некоторого класса блоков разбиений $\mathbf{W}$ и наборов номеров таких блоков используется в методе усечённых разностей — в одном из наиболее распространённых обобщений разностного метода [2–6]. В этом случае неявно полагают, что для итеративных $\otimes$-марковских алгоритмов шифрования вероятность $\mathbf{P}\left\{\left(A_{j^{(0)}}, \ldots, A_{j^{(l)}}\right)\right\}$ набора усечённых разностей $\left(A_{j^{(0)}}, \ldots, A_{j^{(l)}}\right)$ находится как $\prod\limits_{i=0}^{l-1} p_{j^{(i)}, j^{(i+1)}}\left(g^{(i+1)}\right)$, где $A_{j^{(i)}}$ — блок некоторого разбиения множества $X^{\times}$; $p_{j^{(i)}, j^{(i+1)}}\left(g^{(i+1)}\right)$ — вероятность перехода блока $A_{j^{(i)}}$ в блок $A_{j^{(i+1)}}$ под действием раундовой функции $g^{(i+1)}$ в предположении, что раундовый ключ выбирается случайно и равновероятно из множества $K^{(i)}$, $i = 0, \ldots, l$. В ряде работ (см., например, [3, 5]) при применении метода усечённых разностей происходит проверка корректности равенства

$$\mathbf{P}\left\{\left(A_{j^{(0)}}, \ldots, A_{j^{(l)}}\right)\right\} = \prod_{i=0}^{l-1} p_{j^{(i)}, j^{(i+1)}}\left(g^{(i+1)}\right) \tag{1}$$

посредством вычислительных экспериментов. Так, в [5] показано, что экспериментальная оценка вероятности $\mathbf{P}\left\{\left(A_{j^{(0)}}, \ldots, A_{j^{(l)}}\right)\right\}$ может быть больше найденной по формуле (1).

В XSL-алгоритмах блочного шифрования и алгоритмах шифрования Фейстеля с XSL-функцией усложнения марковость последовательности случайных величин $W_{t_0}, \ldots, W_{t_{l-1}}$ определяется свойствами s-боксов. Поэтому в качестве примеров в данной работе приведены преобразования, основанные на операциях экспоненцирования и логарифмирования в кольце вычетов $\mathbb{Z}_n$ (с операцией сложения $+$) и поле $\mathrm{GF}(n+1)$, а также указаны разбиения $\mathbf{W}$, при которых данные преобразования являются $+_{\mathbf{W},\mathrm{ch}}$-марковскими. К этим преобразованиям относятся подстановки s-боксов алгоритма блочного шифрования SAFER [7], экспоненциальные подстановки [8] и логарифмические подстановки. Логарифмические подстановки были предложены первым автором данной работы и М. Е. Масленниковым. Они применяются в семействе функций хеширования MCSSHA, причём первая функция хеширования этого семейства MCSSHA-1

являлась кандидатом для участия в конкурсе SHA-3. Перемешивающие свойства логарифмических подстановок рассматривались, например, в [9].

Пусть $\mathbb{Z}$ — множество всех целых чисел, $\mathbb{Z}_n = \{0, \ldots, n-1\}$. Для $a \in \mathbb{Z}$ через $a_{(d)}$ обозначим такой наименьший элемент $a_{(d)} \in \{0, \ldots, d-1\}$, что $a_{(d)} \equiv a \pmod{d}$. Пусть также $n \in \mathbb{N}$, $n+1$ — простое число, θ — примитивный элемент поля Галуа $\mathrm{GF}(n+1)$ и подстановка $\mu_{\theta,\delta,c} \in S(\mathbb{Z}_n)$ задана условием

$$\mu_{\theta,\delta,c} : x \mapsto \left(\theta^{x+c} \bmod (n+1) + \delta\right)_{(n)}, \ \delta, c \in \mathbb{Z}_n.$$

Утверждение 2. Пусть $m \geqslant 1$, $n = 2^m$ и матрица $\mathbf{p}(b)$ вероятностей переходов разностей подстановки $b \in S(\mathbb{Z}_n)$ такова, что справедливо одно из условий:

1) $p_{i,j}(u) = p_{2^m-i,2^m-j}(b)$ для каждых $i, j \in \mathbb{Z}_n^\times$;
2) $p_{i,j}(b) = p_{2^m-i,j}(b)$ для каждых $i, j \in \mathbb{Z}_n^\times$.

Тогда подстановка b является $+_{\mathbf{W},\mathrm{ch}}$-марковской для разбиения $\mathbf{W} = \{W_0, W_1, \ldots, W_{2^{m-1}}\}$, где

$$W_i = \begin{cases} \{i, 2^m - i\}, & \text{если } i \in \{1, \ldots, 2^{m-1}-1\}, \\ \{i\}, & \text{если } i \in \{0, 2^{m-1}\}. \end{cases}$$

Из утверждения 2 следует $+_{\mathbf{W},\mathrm{ch}}$-марковость подстановки $\mu_{\theta,\delta,0}$ для $\mathbf{W}$-разбиения, так как для произвольных $\varepsilon, \lambda \in \mathbb{Z}_n^\times$ справедливы равенства

$$p_{\varepsilon,\lambda}(\mu_{\theta,\delta,0}) = p_{\varepsilon,2^m-\lambda}(\mu_{\theta,\delta,0}), \quad p_{\varepsilon,\lambda}(\mu_{\theta,\delta,0}) = p_{2^m-\varepsilon,\lambda}(\mu_{\theta,\delta,0}).$$

Из утверждения 2 также следует $+_{\mathbf{W},\mathrm{ch}}$-марковость класса экспоненциальных подстановок $\mu'_\theta : \mathbb{Z}_{2^m} \mapsto \mathrm{GF}(2^m)$, заданных условием

$$\mu'_\theta : \alpha \mapsto \begin{cases} 0, & \text{если } \alpha = 0, \\ \theta^\alpha, & \text{если } \alpha \neq 0, \end{cases}$$

где θ — примитивный элемент поля $\mathrm{GF}(2^m)$.

ЛИТЕРАТУРА

1. *Lai X., Massey J. L., and Murphy S.* Markov ciphers and differential cryptanalysis // EUROCRYPT'1991. LNCS. 1991. V. 547. P. 17–38.
2. *Knudsen L. R.* Truncated and higher order differentials // FSE'1995. LNCS. 1995. V. 1008. P. 196–211.
3. *Matsui M. and Tokita T.* Cryptanalysis of a reduced version of the block cipher E2 // FSE'1999. LNCS. 1999. V. 1636. P. 71–80.
4. *Moriai S., Sugita M., Aoki K., and Kanda M.* Security of E2 against truncated differential cryptanalysis // SAC'1999. LNCS. 2000. V. 1758. P. 106–117.
5. *Reichardt B. and Wagner D.* Markov truncated differential cryptanalysis of Skipjack // SAC'2002. LNCS. 2003. V. 2595. P. 110–128.
6. *Blondeau C.* Improbable differential from impossible differential: on the validity of the model // INDOCRYPT'2013. LNCS. 2013. V. 8250. P. 149–160.
7. *Massey J. L.* SAFER K-64: One year later // FSE'1994. LNCS. 1995. V. 1008. P. 212–232.
8. *Агиевич С. В., Афоненко А. А.* Экспоненциальные s-блоки // Материалы конф. МаБит. М.: МЦНМО, 2003. С. 127–130.
9. *Шемякина О. В.* Об оценке характеристик разбиений различных алгебраических структур // Сб. трудов конф. ИБРР-2011. СПб.: СПОИСУ, 2011. С. 137.