биение U порождает метрику на X, где $X^\times = X\backslash\{e\}$, e — единичный элемент абелевой группы $(X, \otimes)$ с бинарной операцией $\otimes$. Близкими к таким разбиениям являются W-разбиения, где под W-разбиением понимается разбиение множества X на блоки одинаковой мощности. В частности, если W_0 — произвольная подгруппа $(X, \otimes)$, то рассматриваемым W-разбиением является множество смежных классов группы $(X, \otimes)$ по подгруппе W_0. Заметим, что при рассмотрении разбиения $\{W_0\backslash\{e\}, \ldots, W_{r-1}\}$ естественным образом получается $U^{(\mu)}$-разбиение. Кроме того, W-разбиения позволяют для XSL-алгоритмов блочного шифрования учитывать не только строение слоя наложения ключа, но и строение линейного слоя. Например, это возможно, если W_0 — инвариантное подпространство линейного преобразования. Блоки $U^{(\mu)}$-разбиения интерпретируются как множества разностей пар открытого текста (шифртекста). Заметим, что разбиение $X^\times$ с блоками единичной длины применяется в разностном методе, а усечённые разности естественным образом задают W-разбиение.

Показано, что такие укрупнения состояний цепи Маркова, порождённые последовательностями промежуточных шифртекстов i-го раунда, $i = 1, 2, \ldots$, алгоритмов блочного шифрования, являются цепью Маркова. Для них выполнен перенос ряда результатов работы [4]. В частности, приведены условия, при которых алгоритмы блочного шифрования на основе схем XSL, Фейстеля и Лея — Месси [5] являются марковскими относительно рассматриваемых разбиений.

ЛИТЕРАТУРА

1. *Minier M. and Gilbert H.* Stochastic cryptanalysis of Crypton // FSE'00. LNCS. 2000. V. 1978. P. 121–133.
2. *Matsui M.* Linear cryptanalysis method for DES cipher // Eurocrypt. LNCS. 1993. V. 765. P. 386–397.
3. *Biham E. and Shamir A.* Differential Cryptanalysis of the Data Encryption Standard. Springer Verlag, 1993.
4. *Lai X., Massey J. L., and Murphy S.* Markov ciphers and differential cryptanalysis // Eurocrypt. LNCS. 1991. V. 547. P. 17–38.
5. *Vaudenay S.* On the Lai — Massey scheme // Asiacrypt. LNCS. 1999. V. 1716. P. 8–19.

УДК 519.7

О ВЕРОЯТНОСТЯХ r-РАУНДОВЫХ ПАР РАЗНОСТЕЙ XSL-АЛГОРИТМА БЛОЧНОГО ШИФРОВАНИЯ МАРКОВА С ПРИВОДИМЫМ ЛИНЕЙНЫМ ПРЕОБРАЗОВАНИЕМ

М. А. Пудовкина

Раундовая функция XSL-алгоритма блочного шифрования является композицией трёх преобразований: преобразования сдвига (сложение с ключом), нелинейного преобразования (s-бокса) и линейного преобразования. Для XSL-алгоритма блочного шифрования Маркова с приводимым линейным преобразованием вместо «классической» r-раундовой разностной характеристики в разностном методе рассматривается r-раундовая характеристика, заданная последовательностью смежных классов инвариантного подпространства линейного преобразования.

Ключевые слова: *алгоритм шифрования Маркова, инвариантное множество, приводимое линейное преобразование, разностная характеристика.*

Пусть V_n — пространство n-мерных векторов над полем $\mathrm{GF}(2)$ с операцией векторного сложения $\oplus$; $x_1, \ldots, x_t \in_U X$ — элементы $x_1, \ldots, x_t$ выбираются случайно равновероятно и независимо из множества X; $S(X)$ — симметрическая группа на множестве X; $\alpha^g = \alpha g = g(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $g \in S(X)$; $X^\times = X \backslash \{\overrightarrow{0}\}$, $X \subseteq V_n$; $n = d \cdot m$, $\tilde{s} \in S(V_m)$, $h \in \mathrm{GL}_n(2)$, $s = (\tilde{s}_{d-1}, \ldots, \tilde{s}_0) \in S(V_m)^d$, где $s : \alpha \mapsto (\tilde{\alpha}_{d-1}^{\tilde{s}}, \ldots, \tilde{\alpha}_0^{\tilde{s}})$.

Рассмотрим XSL-алгоритм блочного шифрования Маркова с раундовой функцией $g_{k^{(i)}} \in S(V_n)$, заданной как

$$g_{k^{(i)}} : \alpha \mapsto \left(\alpha \oplus k^{(i)}\right)^{sh},$$

где $k^{(i)}$ — n-битный раундовый ключ i-го раунда, $i \in \mathbb{N}$.

Для преобразования $b \in S(V_n)$ и векторов $\varepsilon, \delta \in V_n$ положим

$$p_{\varepsilon,\delta}^{[n]}(b) = 2^{-n} \left| \left\{ \beta \in V_n | (\beta \oplus \varepsilon)^b \oplus \beta^b = \delta \right\} \right|.$$

Заметим, что для векторов $\varepsilon = (\tilde{\varepsilon}_{d-1}, \ldots, \tilde{\varepsilon}_0) \in V_m^d$, $\delta = (\tilde{\delta}_{d-1}, \ldots, \tilde{\delta}_0) \in V_m^d$ справедливо равенство

$$p_{\varepsilon,\delta}^{[n]}(s) = \prod_{i=0}^{d-1} p_{\tilde{\varepsilon}_i,\tilde{\delta}_i}^{[m]}\left(\tilde{s}^{(i)}\right).$$

Пусть $k \in_U V_n$ и α — произвольный фиксированный вектор из V_n. Тогда для векторов $\varepsilon, \delta \in V_n^\times$ положим

$$p_{\varepsilon,\delta}(g|\alpha) = \mathbf{P}\left\{\alpha^{g_k} \oplus (\alpha \oplus \varepsilon)^{g_k} = \delta\right\}.$$

Из определения алгоритма блочного шифрования Маркова [1] следует, что $p_{\varepsilon,\delta}(g) = p_{\varepsilon,\delta}(g|\alpha)$.

Множество Λ, $\Lambda \subset V_n^\times$, назовём *инвариантным* относительно линейного преобразования h, если $\Lambda^h = \Lambda$.

Пусть $\Lambda_0 = \Lambda \cup \{\overrightarrow{0}\}$, Λ_0 — инвариантное подпространство преобразования h в V_n, $b_{\Lambda_0} = \dim \Lambda_0$ и $\Lambda_\delta = \Lambda_0 \oplus \delta$, $\delta \in V_n^\times$. Положим $\theta_0 = \overrightarrow{0}$ и Λ_{θ_i} — i-й смежный класс V_n по Λ_0, $i = 0, \ldots, 2^{n-b_{\Lambda_0}} - 1$.

Зафиксируем произвольные взаимно однозначные отображения

$$\varphi_{\Lambda_{\theta_q}} : \Lambda_{\theta_q} \to \{1, \ldots, |\Lambda_{\theta_q}|\}, \quad i = 1, \ldots, 2^{n-b_{\Lambda_0}} - 1.$$

Смежным классам Λ_θ, Λ_δ поставим в соответствие $|\Lambda_\theta| \times |\Lambda_\delta|$-матрицу $\tilde{\mathbf{q}}_{\Lambda_\theta,\Lambda_\delta} = \left(\tilde{q}_{i,j}^{[\theta,\delta]}\right)$, где $\tilde{q}_{i,j}^{[\theta,\delta]} = p_{\varphi^{-1}(i),\varphi^{-1}(j)^{h^{-1}}}^{[n]}(s)$.

В этом случае для нахождения r-раундовой разностной характеристики рассмотрим последовательность номеров смежных классов $\bar{\theta} = (\theta_{i_0}, \theta_{i_1}, \ldots, \theta_{i_r})$ и $|\Lambda_{\theta_{i_0}}| \times |\Lambda_{\theta_{i_r}}|$-матрицу $\tilde{\mathbf{q}}_{\bar{\theta}}^{(r)} = \left(\tilde{q}_{c_1,c_2}^{[\bar{\theta}]}\right)$, где $\tilde{\mathbf{q}}_{\bar{\theta}}^{(r)} = \prod_{j=1}^{r} \tilde{\mathbf{q}}_{\Lambda_{\theta_{i_{j-1}}},\Lambda_{\theta_{i_j}}}$. Тогда вероятность r-раундовой пары разностей $(\lambda, \lambda') \in \Lambda_{\theta_{i_0}} \times \Lambda_{\theta_{i_r}}$ оценивается снизу $\tilde{q}_{\varphi_{\theta_{i_0}}(\lambda),\varphi_{\theta_{i_r}}(\lambda')}^{[\bar{\theta}]}$.

Таким образом, учёт инвариантного подпространства и его смежных классов может позволить улучшить оценки снизу вероятности r-раундовой пары разностей $(\lambda, \lambda') \in \in \Lambda_{\theta_{i_0}} \times \Lambda_{\theta_{i_r}}$ по сравнению с нахождением вероятности «классической» разностной характеристики. Если размерность инвариантного подпространства Λ_0 небольшая, например $\dim \Lambda_0 \leqslant 16$, то данный подход применим на практике. В этом случае в памяти

требуется хранить не больше r матриц из $2^{2b_{\Lambda_0}}$ элементов. Полученные вероятности $\tilde{q}^{[\bar{\theta}]}_{\varphi_{\theta i_0}(\omega_0),\varphi_{\theta i_r}(\omega_r)}$ могут увеличить число атакуемых раундов. Поэтому приведённый подход эффективнее по сравнению со способом нахождения вероятностей «классических» разностных характеристик. Отметим, что аналогичным образом можно рассматривать матрицы, соответствующие объединению нескольких смежных классов или инвариантных непересекающихся подмножеств. Предложенный подход проиллюстрирован на примере инволютивного алгоритма блочного шифрования ISEBERG [2], представленного на конференции FSE в 2004 г. Проведено сравнении полученных результатов с результатами работы [3].

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. *Standaert F. X., Piret G., Rouvroy G., et al.* ICEBERG: an involutional cipher efficient for block encryption in reconfigurable hardware // FSE'2004. LNCS. 2004. V. 3017. P. 279–299.
3. *Sun Y., Wang M., Jiang S., and Jiang Q.* Differential cryptanalysis of reduced-round ICEBERG // AFRICACRYPT'2012. LNCS. 2012. V. 7374. P. 155–171.

УДК 519.7

УСЛОВИЯ СУЩЕСТВОВАНИЯ СОВЕРШЕННЫХ ШИФРОВ С ФИКСИРОВАННЫМ НАБОРОМ ПАРАМЕТРОВ

С. М. Рацеев

Исследуется задача построения совершенных шифров по заданному множеству открытых текстов X, ключей K и распределению вероятностей P_K на множестве ключей. Приводится критерий, позволяющий однозначно определить, существует ли для заданных X, K, P_K совершенный шифр.

Ключевые слова: *шифр, совершенный шифр.*

Пусть X, K, Y — конечные множества открытых текстов, ключей и шифрованных текстов соответственно. Обозначим через $\Sigma_B = (X, K, Y, E, D, P_X, P_K)$ вероятностную модель шифра [1, 2], где E и D — множества правил зашифрования и расшифрования соответственно. Напомним, что шифр Σ_B называется совершенным (по Шеннону), если для любых $x \in X$, $y \in Y$ выполнено равенство $P_{X|Y}(x|y) = P_X(x)$.

Рассмотрим следующую задачу: по заданному множеству открытых текстов X_0 и множеству ключей K_0 с распределением вероятностей P_{K_0} (независимо от P_{X_0}) однозначно определить, существует ли шифр $\Sigma_B = (X_0, K_0, Y, E, D, P_{X_0}, P_{K_0})$, являющийся совершенным. Таким образом, по заданным X_0, K_0, P_{K_0} требуется определить, найдутся ли такие Y, E, D, для которых шифр Σ_B являлся бы совершенным.

Теорема 1. Для заданных X, $|X| = n$, K, P_K существует совершенный шифр

$$\Sigma_B = (X, K, Y, E, D, P_X, P_K)$$