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

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

тогда и только тогда, когда найдётся такое натуральное число s и n таких разбиений множества K

$$\begin{aligned} &K = K_{11} \cup K_{12} \cup \ldots \cup K_{1s}, \quad K_{1i} \cap K_{1j} = \varnothing, \quad 1 \leqslant i < j \leqslant s, \\ &K = K_{21} \cup K_{22} \cup \ldots \cup K_{2s}, \quad K_{2i} \cap K_{2j} = \varnothing, \quad 1 \leqslant i < j \leqslant s, \\ &\ldots \\ &K = K_{n1} \cup K_{n2} \cup \ldots \cup K_{ns}, \quad K_{ni} \cap K_{nj} = \varnothing, \quad 1 \leqslant i < j \leqslant s, \end{aligned} \tag{1}$$

для которых выполнены следующие условия:

1) $K_{it} \cap K_{jt} = \varnothing$, $1 \leqslant i < j \leqslant n$, $t = 1, \ldots, s$;
2) для любых $1 \leqslant i < j \leqslant n$, $t = 1, \ldots, s$ выполнено равенство

$$\sum_{k \in K_{it}} P_K(k) = \sum_{k \in K_{jt}} P_K(k).$$

Пусть для некоторого числа s выполнены равенства (1) и условия 1 и 2 теоремы. Тогда матрица зашифрования A для (совершенного) шифра Σ_B строится следующим образом. Пусть $Y = \{y_1, \ldots, y_s\}$ — некоторое множество шифрованных текстов, где s — число частей разбиений из (1). Составим матрицу зашифрования размера $|K| \times |X|$, где строки пронумерованы элементами множества K, а столбцы — элементами множества X, следующим образом. В i-м столбце ($i = 1, \ldots, |X|$) данной матрицы в строках, пронумерованных элементами множества K_{ij}, поставим элемент y_j, $j = 1, \ldots, s$.

Следствие 1. Пусть для заданных X, K, P_K существует совершенный шифр. Тогда для любого множества открытых текстов $\widetilde{X}$, $|\widetilde{X}| \leqslant |X|$, и для заданных K, P_K существует совершенный шифр.

Следствие 2. Для заданных X, $|X| = n$, K, P_K, Y, $|Y| = s$, существует совершенный шифр $\Sigma_B = (X, K, Y, E, D, P_X, P_K)$ тогда и только тогда, когда найдётся n таких разбиений (1), для которых выполнены условия 1 и 2 теоремы 1.

Следствие 3. Для заданных K, P_K существует совершенный шифр Σ_B тогда и только тогда, когда найдутся такие n и s, $n \leqslant s$, и такие разбиения (1), для которых выполнены условия 1 и 2 теоремы 1.

Пусть P_{im} — вероятность успеха имитации, P_{podm} — вероятность успеха подмены шифрованного сообщения для шифра Σ_B.

Следствие 4. Пусть для шифра Σ_B (с матрицей зашифрования A) выполнены равенства (1) с условиями 1 и 2 теоремы 1. Тогда

$$P_{\text{im}} = n \max_{1 \leqslant i \leqslant s} \sum_{k \in K_{1i}} P_K(k),$$

$$P_{\text{podm}} = \frac{1}{n} \max_{\substack{1 \leqslant i, j \leqslant s \\ i \neq j}} \frac{\sum\limits_{k \in K_i \cap K_j} P_K(k)}{\sum\limits_{k \in K_{1i}} P_K(k)},$$

где $K_i = \bigcup\limits_{j=1}^{n} K_{ji}$, $i = 1, \ldots, s$.

Отметим, что некоторый интерес представляют совершенные шифры с дополнительными условиями, например условиями имитостойкости. О таких шифрах можно посмотреть в работах [2–4].

ЛИТЕРАТУРА

1. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2005. 480 с.
2. *Зубов А. Ю.* Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005. 192 с.
3. *Рацеев С. М.* О совершенных имитостойких шифрах // Прикладная дискретная математика. 2012. № 3 (17). С. 41–47.
4. *Рацеев С. М.* О совершенных имитостойких шифрах замены с неограниченным ключом // Вестник Самарского государственного университета. Естественнонаучная серия. 2013. № 9/1 (110). С. 42–48.

УДК 512.62

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ АНАЛОГА СХЕМЫ ДИФФИ — ХЕЛЛМАНА, ИСПОЛЬЗУЮЩЕГО СОПРЯЖЕНИЕ И ВОЗВЕДЕНИЕ В СТЕПЕНЬ, НА МАТРИЧНОЙ ПЛАТФОРМЕ[1]

В. А. Романьков

Доказано, что смешанный обобщённый вариант протокола Диффи — Хеллмана на матричной платформе, использующий одновременное возведение в степень и сопряжение фиксированной матрицы, в генерическом случае допускает вычисление разделённого ключа за полиномиальное время, если соответствующая кратная задача дискретного логарифма решается за полиномиальное время. Алгоритм вычисления использует разработанный автором метод линейного разложения, позволяющий находить разделённый ключ без решения задачи поиска сопрягающих элементов, и подход Менезеса с соавт., сводящий вычисление степени матрицы к решению кратной задачи дискретного логарифма. Комбинация этих двух подходов не может использоваться напрямую. Доказательство основного утверждения требует анализа содержаний мономиальных матриц в смежных классах по перестановочным подгруппам группы матриц. Это, в свою очередь, требует изучения аналогичного вопроса для групп подстановок. Последнее облегчается тем, что имеется ряд известных утверждений на эту тему.

Ключевые слова: *криптоанализ, проблема поиска, сопряжение, протокол Диффи — Хеллмана.*

Идея реализации протокола Диффи — Хеллмана на различных платформах, отличных от классических мультипликативных групп конечных полей и завоевавших признание групп эллиптических кривых, использована в целом ряде работ. Чаще всего в качестве платформы выбирались матричные группы, также предлагались конечные и абстрактные бесконечные группы, почти всегда допускающие точное представление матрицами над полем (кроме конечных — это свободные, конечно порождённые нильпотентные и метабелевы, а также полициклические группы, группы кос Артина и т. п.). В данной работе мы ограничимся рассмотрением матричного случая. В начальный период схема Диффи — Хеллмана просто переносилась с мультипликативной группы поля на матричную группу, то есть фиксировался элемент g матричной группы G, первый из корреспондентов (Алиса) выбирал случайное натуральное число k и посылал по открытой сети степень g^k, второй корреспондент (Боб) аналогично выбирал l и посылал g^l. После этого Алиса и Боб легко вычисляли общий ключ g^{kl}.

[1]Работа поддержана грантом РФФИ, проект № 13-01-00239-а.