УДК 621. 391:519.2:519.7

БЛОЧНЫЕ СИММЕТРИЧНЫЕ ШИФРЫ И МАРКОВСКИЕ ПРОЦЕССЫ

И.В. ЛИСИЦКАЯ, В.И. ДОЛГОВ

Обсуждаются известные определения Марковских шифров. Представляется уточнённый подход к их определению, основывающийся на стохастических уравнениях Марковских процессов. Показано, что в соответствии с введенным определением практически любой итеративный шифр является Марковским, в частности, SPN шифры формируют в результате зашифрования Марковские процессы первого порядка, в то время как шифры, построенные с использованием Фестель подобных схем формирования цикловых функций, создают в результате зашифрования Марковские процессы второго порядка. Уточняются некоторые определения, связанные с Марковскими шифрами.

Ключевые слова: Марковский процесс, итеративный *r*-цикловый шифр, Марковская цепь.

ВВЕДЕНИЕ

В качестве введения мы здесь напомним небольшую работу, подготовленную ещё в 1978 году [1]. В этой работе излагаются некоторые важные свойства дискретных и одновременно Марковских процессов, не освещённых в достаточной степени в литературе. Мы приведём некоторые сведения из этой работы, которые будут необходимы в дальнейшем.

В работе вводится понятие Марковского дискретного процесса *k*-того порядка. Рассматривается выборка процесса $y(t_i)$, $i=1,2\ldots,n$, заданного в виде последовательности $y_1, y_2, \ldots, y_n$ выборочных (или средних за элементарный интервал дискретности) значений исходного непрерывного процесса $y(t)$, заданного на некотором конечном интервале времени (T_1, T_2). Отмечается, что наиболее полной статистической характеристикой этого процесса является многомерный закон распределения вероятностей $P(y_1, y_2, \ldots, y_n)$ совокупности его выборочных значений. Определяется понятие Марковского процесса *k*-того порядка. Мы его здесь напомним.

Определение. *Марковским процессом k-того порядка называется процесс, условный закон распределения вероятностей выборочных значений которого для каждого значения выборки y_l, относительно предыдущих значений $y_{l-1}, y_{l-2}, \ldots, y_1$ при любом $l > k$ зависит только от k предшествующих значений, т.е.*

$$P(y_l / y_{l-1}, y_{l-2}, \ldots, y_1) = P(y_l / y_{l-1}, y_{l-2}, \ldots, y_{l-k}) .$$

Показано, что Марковский и одновременно нормальный процесс математически описывается стохастическим дифференциальным уравнением соответствующего порядка, дискретным аналогом которого является линейное неоднородное разностное уравнение со случайной правой частью [2]:

$$y_l + \sum_{p=1}^{k} a_p y_{l-p} = \eta_l \text{ , для } l > k,\ a_p = a_p^{(l)} . \qquad (1)$$

Отметим, что при $l \le k$ имеем начальные условия

$$y_l + \sum_{p=0}^{l-1} a_p^{(l)} y_{l-p} = \eta_l ,\ \ a_0^{(l)} = 0 .$$

В (1) η_l – отсчёт (выборочное значение) случайного δ-коррелированного процесса с нулевым математическим ожиданием и фиксированной дисперсией.

Нас далее будут интересовать сначала Марковские процессы первого порядка ($k = 1$), для которых

$$P(y_l /, y_{l-1}, y_{l-2}, \ldots, y_1) = P(y_l /, y_{l-1}) . \qquad (2)$$

В [1] показано, что простейший Марковский процесс первого порядка (экспоненциально коррелированный нормальный процесс) описывается стохастическим разностным уравнением:

$$y_l = -e^h y_{l-1} + \eta_l , \qquad (3)$$

где $h = \dfrac{T_0}{\tau_k}$ (T_0 – интервал дискретности, τ_k – время корреляции процесса). Ему соответствует в непрерывном времени стохастическое дифференциальное уравнение первого порядка, но нас будет интересовать именно представление, связывающее текущее значение дискретного процесса y_l с предыдущим отсчётным значением y_{l-1}.

Прежде чем идти дальше, полезно будет обобщить приведенные выше сведения следующим образом: *для Марковского процесса первого порядка соседние отсчётные значения процесса* (*два соседних значения*) *связаны между собой случайной компонентой, для Марковского процесса второго порядка три смежных отсчётных значения связаны между собой одной или более случайными компонентами, наконец, для Марковского процесса k-того порядка выборка из k + 1-го соседних отсчётных значений процесса связаны между собой случайными компонентами.*

Приведенные сведения и будут той основой, на которой мы будем строить определения для Марковских шифров.

Мы здесь хотим извиниться перед читателями за то, что статья носит больше фрагментарный, чем последовательный характер, но речь здесь идёт об уже вроде бы осознанных и понятных многим специалистам положениях, которые мы пытаемся уточнить (углубить их понимание).

1. ОБЗОР ПУБЛИКАЦИЙ ПО МАРКОВСКИМ ШИФРАМ

Напомним сначала положения, относящиеся к Марковским шифрам, которые приведены в немногочисленных публикаций в этом направлении. Основополагающей здесь, по-видимому, следует считать совместную работу Лэя, Мэсси и Марфу [3] 1991 года.

В этой работе рассматривается итеративный *r*-цикловый шифр, представленный авторами в виде рис. 1, на котором приведены необходимые нам обозначения.

Приводится такое определение Марковского шифра.

Определение. *Итеративный шифр с цикловой функцией* $Y = f\{X, Z\}$ *является Марковским шифром, если имеется групповая операция* $\otimes$, *определяющая дифференциал такая, что для всех значений* α ($\alpha \neq 0$) *и* β ($\beta \neq 0$) *условная вероятность*

$$P(\Delta Y = \beta \,|\, \Delta X = \alpha, X = \gamma)$$

является независимой от γ, *когда подключ* Z *является равномерно случайным.*

Далее приводится названная решающей теорема 2, которая объясняет, как указывают авторы, терминологию «Марковский шифр».

Теорема 2. *Если r-цикловый итеративный шифр является Марковским шифром и r цикловых ключей являются независимыми и равномерно распределёнными* (*случайными*), *то последовательность разностей* $\Delta X = \Delta Y(0)$, $\Delta Y(1), \ldots, \Delta Y(r)$ *является однородной Марковской цепью. Более того, эта Марковская цепь является стационарной, если разности* ΔX *являются равномерно распределёнными над ненулевыми элементами группы.*

В этой работе шифр с операцией, определяющей разности, рассматривается как группа, ΔX является входной разностью, а $\Delta Y(i)$, $i = 1, 2, \ldots, r$ – поцикловые выходные разности.

В качестве примера Марковского шифра приводится шифр DES. Отмечается, что для Марковского шифра с независимыми и равномерно распределёнными (случайными) цикловыми подключами вероятность *r*-цикловой дифференциальной характеристики определяется уравнением Чепмена-Колмогорова для Марковской цепи:

$$P\left(\Delta Y(1) = \beta_1, \Delta Y(2) = \beta_2, \ldots, \Delta Y(r) = \beta_r, \Delta X = \beta_0\right) = \prod_{i=1}^{r} P\left(\Delta Y(1) = \beta_1 \,|\, \Delta X = \beta_{i-1}\right).$$

Из этого следует, что вероятность *r*-циклового дифференциала (β_{01}, β_r) есть

$$P\left(\Delta Y(r) = \beta_r \,|\, \Delta X = \beta_0\right) = \sum_{\beta_1}\sum_{\beta_2}\cdots\sum_{\beta r-1}\prod_{i=1}^{r} P\left(\Delta Y(1) = \beta_1 \,|\, \Delta X = \beta_{i-1}\right),$$

где суммы рассматриваются над всеми возможными значениями разностей между различными элементами, т.е. над всеми элементами группы, исключая нейтральный элемент *e*.

Заметим здесь, что в теореме 2 и последующих разъяснениях говорится о Марковских шифрах с независимыми и равномерно распределёнными (случайными) цикловыми подключами. Как станет понятно из дальнейшего, само понятие Марковского шифра включает отмеченные выше свойства цикловых подключей, так что специальное оговаривание для Марковского шифра независимости и случайности цикловых подключей является, конечно, лишним, т.е. аккуратнее было бы говорить от том, что итеративный шифр является Марковским, если *цикловые подключи являются независимыми и равномерно распределёнными.*

Полезно будет напомнить здесь также гипотезу статистической эквивалентности, представленную авторами в рассматриваемой работе:

Гипотеза статистической эквивалентности: *Для* $(r-1)$*-циклового дифференциала* (α, β)

$$P\{\Delta Y(r-1) = \beta \,|\, \Delta X = \alpha) \approx P\{\Delta Y(r-1) = \beta \,|\, \Delta X = \alpha, Z^{(1)} = \omega_1, \ldots, Z^{(r-1)} = \omega_{r-1}\}$$

почти для всех подключевых значений $(\omega_1, \ldots, \omega_{r-1})$.

Эта гипотеза в работе используется для обоснования условий уязвимости итеративного шифра к атакам дифференциального криптоанализа. Нам она понадобится для обоснования другого факта. Мы далее покажем, что эта гипотеза выполняется для всех итеративных шифров, достигших стационарного состояния.

Приведём также теорему 3 этой работы:

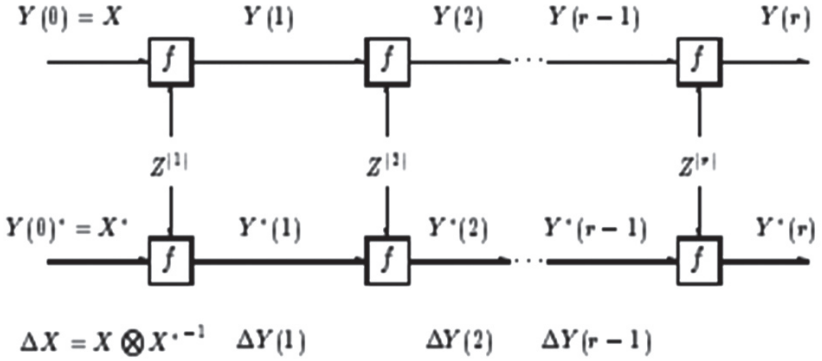

Рис. 1. Шифрование пары плайнтектов в *r*-цикловом итеративном шифре

Теорема 3. *Для Марковского шифра блочной длины m с независимыми и равномерно распределёнными цикловыми подключами, если полубесконечная Марковская цепь* $\Delta X = \Delta Y(0), \Delta Y(1), \ldots$ *имеет «равномерно-устойчивое вероятностное» распределение, т.е. существует вероятностный вектор* $(p_1, p_2, \ldots, p_M)$ *такой, что для всех* α_i

$$\lim_{r\to\infty} P\left(\Delta Y(r) = \alpha_j \mid \Delta X = \alpha_i\right) = p_j,$$

то это равномерно-устойчивое распределение должно быть равномерным $(1/M, 1/M, \ldots, 1/M)$, т.е. $\lim_{r\to\infty} P\left(\Delta Y(r) = \alpha_j \mid \Delta X = \alpha_i\right) = \frac{1}{2^m - 1}$ для каждого дифференциала (α, β), так что каждый дифференциал является, грубо говоря, равно вероятным для достаточно большого числа циклов. Если мы предполагаем дополнительно, что для этого Марковского шифра выполняется гипотеза статистической эквивалентности, то для почти всех подключей этот шифр безопасный против атаки дифференциального криптоанализа после достаточного числа циклов [3].

Мы далее покажем, что первая часть утверждения этой теоремы не соответствует реальному состоянию дел, не говоря уже о том, что гипотеза статистической эквивалентности выполняется для Марковских шифров безусловно.

Приведём также выдержки из другой работы [4], в которой затрагиваются Марковские шифры. Это работа авторов L. Keliher-a, H. Meijer-a и S. Tavares-a. Мы далее привязываемся к обозначениям именно этой работы.

В [4] *R*-цикловый шифр определяется аналитически как отображение $\varepsilon : \{0,1\}^N \to \{0,1\}^N$, для которого цикл *r* задается функцией $\mathbf{y} = \varepsilon_r\{\mathbf{x}; \mathbf{k}^r\}$; $\mathbf{x} : \{0,1\}^N$ является цикловым входом, $\mathbf{k}^r : \{0,1\}^N$ является подключом *r*-того цикла. Тогда, отмечается в этой работе, при применении для сложения с ключом групповой операции XOR ($\oplus$) над $\{0,1\}^N$ *R*-цикловый шифр ε является Марковским шифром, если для $1 \le r \le R$ и любых $\mathbf{x}, \Delta\mathbf{x}, \Delta\mathbf{y} \in \{0,1\}^N$,

$$\begin{aligned}&\mathrm{Prob}_{\mathbf{K}}\{\varepsilon_r(\mathbf{x};\mathbf{K}) \oplus \varepsilon_r(\mathbf{x} \oplus \Delta\mathbf{x};\mathbf{K}) = \Delta\mathbf{y}\} = \\ &= \mathrm{Prob}_{\mathbf{X},\mathbf{K}}\{\varepsilon_r(\mathbf{X};\mathbf{K}) \oplus \varepsilon_r(\mathbf{x} \oplus \Delta\mathbf{x};\mathbf{K}) = \Delta\mathbf{y}\},\end{aligned} \quad (4)$$

где **X** и **K** независимые случайные значения, равномерно распределенные над $\{0,1\}^N$ и **K** множество всех независимых ключей соответственно.

Соотношение (4), отмечают авторы, определяет вероятность для ключа, который фиксированное входное различие преобразует в фиксированное выходное различие, не зависящие от циклового входа.

Легко показать, отмечается также в этой работе, что SPN шифры с фиксированными S-блоками являются Марковскими шифрами.

Из представленных материалов следует, что все подходы к заданию (описанию) Марковских шифров связываются с уравнениями для дифференциалов, что, как мы покажем далее, является не совсем аккуратным. Кроме того, ряд из представленных утверждений, как видно из замечаний, представленных по тексту, представляются не совсем корректными. Мы в этой и последующей работе поставили задачу более строгого обоснования Марковских шифров и уточнения ряда принципиальных моментов, связанных с ними.

2. УТОЧНЁННЫЙ ПОДХОД К ОПРЕДЕЛЕНИЮ МАРКОВСКИХ ШИФРОВ

Первое положение, которое мы хотим здесь сначала обосновать, состоит в том, что практически любой современный шифр является шифром, формирующим в результате выполнения процедуры зашифрования Марковский процесс.

Мы здесь предлагаем свою, как нам кажется, более строгую (последовательную) точку зрения к определению Марковских шифров.

Рассмотрим более детально SPN шифр, представленный на рис. 2, заимствованным из работы [5].

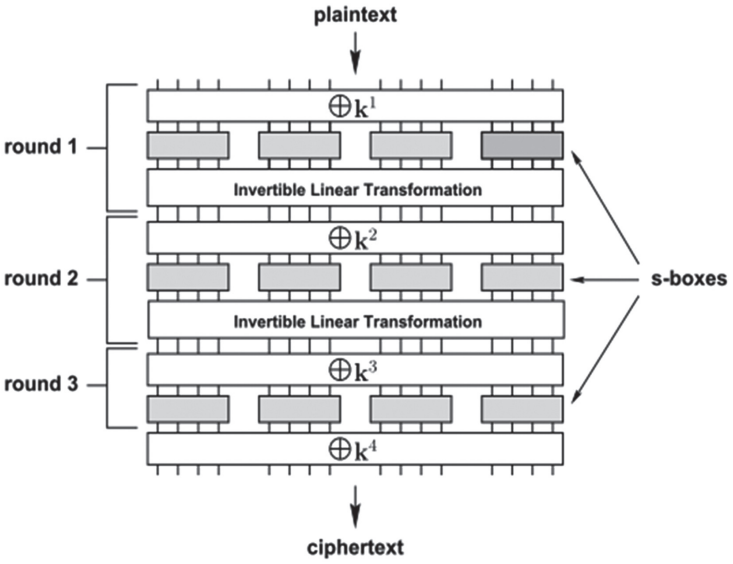

Рис. 2. SPN с $N = 16$, $M = n = 4$, и $r = 3$

Эта r-цикловая подстановочно-перестановочная схема (SPN) требует $r + 1$ N-битных подключей, $\mathbf{k}^1$, $\mathbf{k}^2$, ..., $\mathbf{k}^r$, $\mathbf{k}^{r+1}$. Каждый цикл (раунд) состоит из трёх стадий, или слоёв.

В ключесмешивающей стадии N-битный цикловой выход является *побитным XOR-ом (суммой по модулю два) с подключом для этого цикла.*

В подстановочной стадии результирующий блок делится на M подблоков размера n ($N = Mn$), и каждый подблок становится входом в биективный $n \times n$ подстановочный блок (S-блок) – являющийся биективным отображением из $\{0,1\}^n$ в $\{0,1\}^n$.

В стадии линейного преобразования, выход подстановочной стадии обрабатывается инвертируемым N-битным линейным преобразованием (классическое линейное преобразование было поразрядной перестановкой, откуда и следует появление названия подстановочно-перестановочная схема [6]). Линейное преобразование обычно исключается из последнего цикла, так как легко показать, что его включение в преобразование не добавляет стойкости шифру. Финальный подключ $\mathbf{k}^{r+1}$ XOR-рируется (суммируется по модулю 2) с выходом цикла r чтобы сформировать шифртекст. Предполагается, что те же самые линейные преобразования используются в каждом цикле. Если не оговорено иного, то никаких ограничений не установлено и на выбор S-блоков.

Расшифрование выполняется прогоном SPN «обратно (задом наперед)». Подключ $\mathbf{k}^{r+1}$ сначала XOR-рируется с зашифрованным текстом, и затем в каждом цикле r (из R вплоть до 1-го), выполняется обратное линейное преобразование, сопровождаемое обратными S-блоками, и результирующий блок XOR-рируется с $\mathbf{k}^1$.

Здесь мы подходим к тому, что если выделить в рассмотренном шифре сложение с цикловым подключом в отдельное преобразование (это можно сделать практически в любом SPN шифре), то одноцикловое преобразование такого шифра всегда можно представить в виде результата выполнения над входом в цикловую функцию преобразования F (прохождение через S-блоки и линейное преобразование) и последующего сложения результата преобразования со случайной компонентой, определяемой цикловым подключом, т.е. блок данных на выходе цикловой функции будет иметь вид:

$$\mathbf{y} = \varepsilon_r\{\mathbf{x}; \mathbf{k}^{r+1}\} = F_r\{\mathbf{x}\} + \mathbf{k}^{r+1}. \qquad (5)$$

В результате мы приходим к аналогу уравнения (3), особенностью которого является то, что в уравнении (5) над цикловым входом $\mathbf{x}: \{0,1\}^N$ выполняется преобразование не линейного типа, как это сделано в уравнении (3), а нелинейное преобразование, которое осуществляется в поле $\mathbf{x}, \mathbf{y} \in \{0,1\}^N$. Но это всё равно получается уравнение, связывающее предыдущее значение входа $\mathbf{x}$ с текущим $\mathbf{y}$ (это уже новый вход в очередной цикл) с помощью случайной компоненты $\mathbf{k}^{r+1}$. Если полагать, что ключи для циклов выбираются равновероятно и независимо, то это уравнение Марковского процесса (теперь, конечно же, отличающегося от нормального). В результате предлагается определение Марковского шифра в виде:

Определение 1. *Марковским шифром* (*первого порядка*) *является* (*называется*) *шифр, для которого соотношение для выхода цикловой функции с её входом для любого значения входа и выхода* $\mathbf{x}, \mathbf{y} \in \{0,1\}^N$ *определяется нелинейным уравнением* (5), *в котором случайная компонента в правой части является ключевым значением* $\mathbf{k}^{r+1} \in \{0,1\}^N$, *выбранным независимо и равновероятно из всего множества возможных ключей.*

Можно ввести и определение Марковского шифра k-того порядка:

Определение 1′. *Марковским шифром* (*k-того порядка*) *называется шифр, для которого соседние значения выходов k цикловых функций и значение входа в первую цикловую функцию их этого набора связаны между собой нелинейно случайной компонентой* (*нелинейное уравнение, связывающее $k + 1$ соседних значений на выходах цикловых функций, содержит случайную компоненту*).

В этом случае мы имеем в виду уравнение, которое отличается от (1) нелинейной связью переменных, входящих в него.

Мы здесь привели определение Марковского шифра k-того порядка, так как нам потребуется в рамках этой работы и Марковские шифры второго порядка.

Установим (определим) теперь связь приведенных определений с определениями, известными из литературы.

Для входа в цикловую функцию $\mathbf{x}' = \mathbf{x} \oplus \Delta\mathbf{x}$, с учётом (5) имеем:

$$\mathbf{y}' = \varepsilon_r\{\mathbf{x} \oplus \Delta\mathbf{x}; \mathbf{k}^{r+1}\} = F_r\{\mathbf{x}'\} + \mathbf{k}^{r+1}.$$

В результате для дифференциалов (разностей) циклового преобразования $\mathbf{y} \oplus \mathbf{y}' = \Delta\mathbf{y}_r$, $\mathbf{x} \oplus \mathbf{x}' = \Delta\mathbf{x} = \Delta\mathbf{y}_{r-1}$ для одного и того же ключевого значения $\mathbf{k}^{r+1}$ приходим к уравнению

$$\Delta\mathbf{y}_r = F_r\{\mathbf{x}\} \oplus F_r\{\mathbf{x}'\} = F_r^*\{\Delta\mathbf{x}\} = F_r^*\{\Delta\mathbf{y}_{r-1}\}. \qquad (6)$$

В (6) F_r^* – функция циклового преобразования разностей. В рассмотренных выше и других публикациях [3-8] понятие Марковского шифра связывают именно с уравнением для дифференциалов. Ещё один пример. В [7] Марковским назван шифр, у которого уравнение шифрования на одном цикле удовлетворяет условию: вероятность дифференциала не зависит от выбора открытых текстов. Тогда, если подключи циклов между собой независимы, то последовательность разностей после каждого цикла образует Марковскую цепь, где последующее состояние определяется только предыдущим.

Конечно, это и приведенные выше понятия согласуются с отмеченным определением

Марковского процесса первого порядка для дифференциалов.

Но мы хотим сейчас привлечь внимание к имеющимся в литературе подходам к делению шифров на Марковские и немарковские. Нам представляется, что пропущенная многими авторами связь, выражаемая в виде уравнения, которое оперирует не с дифференциалами, а с соседними значениями одноцикловых переходов шифра, привела к не совсем аккуратной интерпретации свойств некоторых криптографических преобразований.

Так в [8] шифр ГОСТ 28147-89 относится к немарковским. Напомним, что в режиме простой замены шифра ГОСТ-а [9] 64-битный блок открытого текста (сообщения) разбивается на две части по 32 бита каждая (правая половина блока далее обозначена A_0, а левая B_0). Осуществляется 32 однотипных цикла преобразования, структура которых в каждом из циклов описывается выражениями

$$A_i = f(A_{i-1} \left[+\right] K_j) \oplus B_{i-1}, \qquad (7)$$

$$B_i = A_{i-1}, \qquad (8)$$

причем для $i = \overline{1,24}$ берется $j = (i-1) \bmod 8$, для $i = \overline{25,31}$ соответственно $j = 32 - i$, и для последнего цикла

$$A_{32} = A_{31},$$

$$B_{32} = f(A_{31} \left[+\right] K_0) \oplus B_{31},$$

где i – номер итерации; символом $\left[+\right]$ обозначена операция сложения по модулю 2^{32}. Тогда с учётом (8) соотношение (7) можно переписать в виде:

$$A_i = f(A_{i-1} \left[+\right] K_j) \oplus A_{i-2}.$$

Легко убедиться, что по нашему второму определению мы пришли к уравнению Марковского процесса второго порядка (если считать цикловые подключи независимыми), и, следовательно, шифр ГОСТ 28147-89 тоже является Марковским (правда, здесь случайная компонента вошла в нелинейное преобразование). Представляется, что реально существующая корреляция подключей шифра существенно не изменит картину.

Марковским шифром второго порядка является также и шифр DES, для которого уравнения зашифрования (R – правый полублок, L – левый полублок) имеют вид [9]:

$$R_i = f\left(R_{i-1}, K_i\right) \oplus R_{i-2},$$

$$L_i = R_{i-1}.$$

Для $R'_i = f\left(R'_{i-1}, K_i\right) \oplus R'_{i-2}$, где $R'_i = \Delta R \oplus R_i$ имеем:

$$\Delta R_i = f^*\left(\Delta R_{i-1}\right) \oplus \Delta R_{i-2}. \qquad (9)$$

В работе [3] шифр DES причисляется к Марковским шифрам (первого порядка). На самом же деле, это справедливо лишь в том случае, если речь идёт о дифференциальной характеристике, использованной Э. Бихамом и А. Шамиром [10] при построении предложенной ими атаки на шифр, вероятность которой (характеристики) действительно приводится к произведению вероятностей цикловых переходов, характерному для частных дифференциалов Марковских шифров первого порядка. Напомним, что при построении своей атаки они воспользовались трёхблочными характеристиками обнуляющего типа (d = 1960 0000), для которых в (9) надо положить

$$\Delta R_{i-2} = \Delta R_{i-4} = \ldots = \Delta R_{i-2k} = 0,$$

при этом, естественно, что

$$f^*\left(\Delta R_{i-2}\right) = f^*\left(\Delta R_{i-4}\right) = \ldots = f^*\left(\Delta R_{i-2k}\right) = 0.$$

Для характеристик обнуляющего типа соответственно $\Delta R_{i-1} = \Delta R_{i-3} = \ldots = \Delta R_{i-2k-1} = d$, в то время как $f^*\left(\Delta R_{i-1}\right) = f^*\left(\Delta R_{i-3}\right) = \ldots = f^*\left(\Delta R_{i-2k-1}\right) = 0$.

В результате:

$$\Delta R_i = f^*\left(\Delta R_{i-1}\right) = 0 \text{ с вероятностью } p,$$

$$\Delta R_{i-1} = f^*\left(\Delta R_{i-2}\right) \oplus \Delta R_{i-3} \rightarrow \Delta R_{i-1} = \Delta R_{i-3} = d$$
с вероятностью 1,

$$\Delta R_{i-2} = f^*\left(\Delta R_{i-3}\right) = 0 \text{ с вероятностью } p,$$

$$\Delta R_{i-3} = \Delta R_{i-5} = d \text{, с вероятностью } 1 \ldots,$$

т.е. в этом случае мы действительно приходим скорее не к уравнениям дифференциалов Марковского шифра первого порядка, а к результирующей вероятности дифференциальной характеристики выражаемой в виде произведения вероятностей однотипных цикловых переходов (рассматривается частная дифференциальная характеристика), причём половина из них происходят без снижения вероятности (с вероятностью единица).

Но самое интересное, так это то, что и Марковские шифры первого порядка и Марковские шифры второго порядка приходят к одному и тому же стационарному состоянию: таблицы полных дифференциалов и линейных корпусов шифров асимптотически повторяют законы распределения вероятностей XOR переходов и смещений таблиц линейных аппроксимаций случайных подстановок соответствующей степени. Но об этом в следующей публикации.

Возвращаясь к теореме 2, мы здесь хотим обратить внимание на присутствующее в её формулировке требование независимости дифференциалов от выбора открытых текстов (ΔX являются равномерно распределёнными над ненулевыми элементами группы) и утверждение в теореме о стационарности Марковской цепи.

Так вот, если рассматривать теорию Марковских процессов [1 и др.], то любой случайный процесс имеет своё начало и конец. Например, простейший нормальный Марковский процесс

(3) не сразу приобретает показатели стационарного распределения. Начальное его значения следует рассматривать как нестационарное. Для Марковского процесса k-того порядка (см. начальные условия для уравнения (1)) будет уже переходный процесс из k смежных значений (для нормального процесса).

Так и в шифрах. На основе многочисленных результатов проведенных экспериментов мы здесь утверждаем, что большинство современных шифров (использующих для введения циклового подключа не только групповую операцию XOR) являются Марковскими (текущее значение шифртекста является функцией конечного числа предыдущих значений шифртекстов). Для каждого такого шифра существует определённое (небольшое) число начальных циклов, после которого законы распределения переходов XOR таблиц (дифференциалов) приходят к установившемуся (стационарному) значению. На первых шагах шифрования Марковскому шифру присущ переходный период, который вполне согласуется с положениями теории Марковских процессов. Шифр приходит к стационарному процессу (состоянию) асимптотически.

И ещё в отношении равномерности распределения входных разностей ΔX над ненулевыми элементами группы, отмеченными в теореме 2. Дело в том, что уравнение (5) и соответствующее ему уравнение (6) определяют Марковский процесс при любом значении входа $\mathbf{x} \in \{0,1\}^N$. Множество равновероятных значений входов необходимо лишь для формирования закона распределения переходов XOR таблицы шифра, повторяющего распределение дифференциалов случайной подстановки, которое устанавливается после переходного периода.

Остаётся отметить, что после публикации линейного криптоанализа, теория Марковских шифров была распространена на сопротивляемость линейному криптоанализу, что привело к аналогичным выводам для линейных приближений (корпусов) шифров [11]. Для нас в этом нет ничего нового. Наши исследования [12,13 и др.] и в этом случае свидетельствуют, что линейные показатели шифров при росте числа циклов приходят к соответствующим показателям случайных подстановок (Марковский шифр приходит к стационарному состоянию и по этому показателю). Напомним здесь, что равенства, используемые при построении линейных аппроксимаций шифров, определяют связь соседних значений входов и выходов цикловых функций (прошедших соответствующие маски) через случайную компоненту (сумму ключевых битов).

Здесь мы хотим остановиться, хотя у нас есть ещё претензии к использованию матриц переходных вероятностей при оценке показателей стойкости шифрующих преобразований (Марковских шифров), да и в целом к развиваемой во многих работах самой методике оценки стойкости БСШ к атакам дифференциального и линейного криптоанализа. Мы на них остановимся в нашей следующей работе.

ВЫВОДЫ

К основным выводам из представленных в работе результатов, предложений и соображений можно отнести такие:

1. Имеющиеся в литературе подходы к определению Марковских шифров представляются не совсем аккуратными.

2. Предлагается уточнённый подход к определению Марковских шифров, который строится на основе строгого математического определения Марковского случайного процесса k-того порядка.

3. Показано, что в соответствии с введенным определением практически любой итеративный шифр является Марковским, в частности, SPN шифры формируют в результате зашифрования Марковские процессы первого порядка, в то время как шифры, построенные с использованием Фестель подобных схем формирования цикловых функций, создают в результате зашифрования Марковские процессы второго порядка.

4. Для каждого итеративного (Марковского) шифра существует определённое (небольшое) число начальных циклов шифрования, после которого законы распределения переходов XOR таблиц (дифференциалов) и смещений таблиц линейных аппроксимаций (линейных корпусов) шифра приходят к установившемуся (стационарному) значению. На первых шагах шифрования Марковскому шифру присущ переходный период. Шифр приходит к стационарному процессу (состоянию) асимптотически.

Литература

[1] *Долгов В.И.* Вопросы теории и цифрового моделирования нормальных Марковских процессов. / МО. – 1978. – 74 с.

[2] *Иванов В.А.* Математические основы теории автоматического регулирования / В.А. Иванов, Б.К.Чемоданов, В.С. Медведев // Изд-во «Высшая школа». – М., 1971. – 755 с.

[3] *X. Lai, J. Massey, and S. Murphy,* Markov ciphers and differentjal cryptanalysis, Advances in Cryptalogy – EUROCRYPT'93, LNCS 547, Springer-Verlag, pp. 17-38, 1991.

[4] *L. Keliher, H. Meijer, and S. Tavares,* Toward the true random cipher: On expected linear probability values for SPNs with randomly selected s-boxes, chapter in Communications, Information and Network Security, V. Bhargava, H. Poor, V. Tarokh, and S. Yoon (Eds.), pp. 123-146, Kluwer Academic Publishers, 2003.

[5] *F. Sano, K. Ohkuma, H. Shimizu, S. Kawamura.* On the Security of Nested SPN Cipher against the Differential and Linear Cryptanalysis/ IEICE Trans. Fundamentals, vol. E86-a, NO.1 January 2003, pp. 37-46.

[6] *H. Feistel*, Cryptography and computer privacy, Scientific American, Vol. 228, No. 5, pp. 15–23, May 1973.

[7] *L. Keliher,* Linear Cryptanalysis of Substitution-Permutation Networks. A thesis submitted to the School of Computing in conformity with the requirements for the degree of Doctor of Philosophy, 2003, 160 p.

[8] *Ковальчук Л.В.* Сходимость последовательности матриц вероятностей дифференциальных аппроксимаций немарковского блочного шифра к равновероятной матрице при увеличении количества циклов. // Прикладная радиоэлектроника – 2007. – Т.5, № 2 – С. 274-276.

[9] ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

[10] *E. Biham and A. Shamir.* Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology, 4(1): 3-72, 1991.

[11] Joan Daemen, Vincent Rijmen Probability distributions of Correlation and Differentials in Block Ciphers. / Joan Daemen, Vincent Rijmen // April 13, 2006, pp. 1–38.

[12] *Горбенко І.Д.* Новая идеология оценки стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа. / І.Д. Горбенко, В.И. Долгов, И.В. Лисицкая, Р.В. Олейников // Прикладная радиоэлектроника. – 2010. – Т. 9, № 3. – С. 212-320.

[13] *Кузнецов А.А.* Линейные свойства блочных симметричных шифров, представленных на украинский конкурс. / А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника. – 2011. Т. 10, № 2. – С. 135-140.

Поступила в редколлегию 20.02.2012

Лисицкая Ирина Викторовна, кандидат технических наук, доцент кафедры БИТ ХНУРЭ. Область научных интересов: криптография, теория сложности.

Долгов Виктор Иванович, доктор технических наук, профессор кафедры БИТ ХНУРЭ. Область научных интересов: математические методы защиты информации.

УДК 621. 391:519.2:519.7

Блочні симетричні шифри та марковські процеси / І.В. Лисицька, В.І. Долгов // Прикладна радіоелектроніка: наук.-техн. журнал. – 2012. – Том 11. № 2. – С. 137–143.

Обговорюються відомі визначення Марківських шифрів. Наводиться уточнений підхід до їх визначення, що ґрунтується на стохастичних рівняннях Марківських процесів. Показано, що відповідно до введених визначень практично будь-який ітеративний шифр є Марківським, зокрема, SPN шифри формують в результаті зашифрування Марківські процеси першого порядку, в той час як шифри, побудовані з використанням Фестель подібних схем формування циклових функцій, створюють в результаті зашифрування Марківські процеси другого порядку. Уточнюються деякі визначення, пов'язані з Марківськими шифрами.

Ключові слова: Марківский процес; ітеративний *r*-цикловий шифр; Марківський ланцюг.

Іл. 2. Бібліогр. 13 найм.

UDC 621. 391:519.2:519.7

Block symmetric ciphers and Markov processes / I.V. Lysytska, V.I. Dolgov // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 137–143.

The paper discusses the famous definitions of Markov ciphers and provides an updated approach to their definition based on the stochastic equations of Markov processes. It is shown that in accordance with the definition introduced almost any iterative cipher is a Markov one, in particular, SPN ciphers form Markovian first order processes as a result of encoding, while the ciphers, constructed with use of Festel-like schemes of forming cyclic functions, form Markov second order processes as a result of encoding. Some definitions, related to the Markov ciphers, are particularized.

Keywords: Markov process, iterative *r*-round cipher, Markov chain.

Fig. 02. Ref. 13 items.