УДК 681.3.06

АНАЛИЗ ОСНОВНЫХ АТАК НА ТРЁХРАУНДОВУЮ ЦЕПЬ ФЕЙСТЕЛЯ

М.Ф. БОНДАРЕНКО, А.Б. НЕБЫВАЙЛОВ

Анализируются основные атаки на трехраундовую сеть Фейстеля с целью определения отличия такой сети от случайной перестановки на множестве I_{2n}, обсуждаются критерии оценки.

The basic attacks on Feistel's three-round network for the purpose of defining the difference of such a network from a random rearrangement on the set I_{2n} are analyzed, estimation criteria are discussed.

Симметричные блочные шифры являются одним из основных компонентов в современных системах защиты информации. Кроме обеспечения конфиденциальности, они используются как базовый примитив для реализации других криптографических преобразований, в частности, генераторов псевдослучайных последовательностей и алгоритмов выработки кода аутентификации сообщений, протоколов аутентификации. Криптографическая стойкость таких преобразований также практически полностью зависит от свойств базового блочного шифра.

В свою очередь, симметричные блочные алгоритмы шифрования представляют собой достаточно сложные конструкции, как правило, состоящие из последовательного применения нелинейных и линейных операций. Для современных блочных шифров высокоуровневая структура в значительной степени определяет свойства всего криптографического преобразования, включая стойкость к различным методам криптоанализа.

Количество итераций (раундов) шифрования для большинства современных шифров задаётся исходя из свойств циклового преобразования и расчёта стойкости к дифференциальному и линейному криптоанализу. В отличие от этой достаточно формализованной процедуры, выбор конкретной схемы алгоритма шифрования (цепь Фейстеля, SPN-структура или схема Лей-Месси) производится, по большей части, по индивидуальным предпочтениям разработчика, без соответствующего обоснования.

В связи с этим, получение численной оценки эффективности высокоуровневой структуры алгоритма шифрования позволит формализовать и алгоритмизировать процесс разработки симметричных блочных шифров с заданными свойствами. Оценку целесообразно делать, исходя из криптографической стойкости преобразования.

При дальнейшем изложении будут использоваться следующие обозначения:

I_n – множество всех элементов вида $\{0,1\}^n$;

I_{2n} – множество всех элементов вида $\{0,1\}^{2n}$;

$P_n \subset I_n$ – множество перестановок элементов вида $\{0,1\}^n$;

$P_{2n} \subset I_{2n}$ – множество перестановок элементов вида $\{0,1\}^{2n}$;

F_n – множество функций $F: I_n \to I_n$;

F_{2n} – множество функций $F: I_{2n} \to I_{2n}$.

Симметричный блочный шифр может быть представлен в виде отображения $g: I_{2n} \to I_{2n}$ на основе использования случайных функций из F_n [1,2]. В современной криптографии безопасность блочного шифра определятся в терминах вычислительной неразличимости от случайной перестановки при использовании некоторого алгоритма-различителя [1, 2, 4, 5].

В общем случае, задача состоит в том, чтобы дать некоторые оценки вероятности того, что алгоритм-различитель сможет на основании серии из m запросов и соответствующих им ответов выполнить различие между отображением $g: I_{2n} \to I_{2n}$ и случайной функцией из F_{2n}. Следует отметить, что подобные отображения могут быть практически неразличимы от случайной функции из F_{2n} в случае, если алгоритм-различитель имеет доступ только к прямым запросам, и хорошо различимы в случае доступа алгоритма-различителя к обратным запросам [3].

Наиболее широко известной и изученной конструкцией для построения подобных отображений является сеть Фейстеля. В [3] показано, что один раунд сети Фейстеля с использованием случайной функции из F_n является генератором перестановок. Как следствие, применение нескольких раундов сети Фейстеля также является генератором перестановок. В этой связи, проведение различия между перестановками [2,8] и значениями случайной функции, в силу их определения, является некорректным и приводит к заранее известному и прогнозируемому результату [8]. Очевидно, что критерий неразличимости должен быть переопределен в терминах перестановок. Тем не менее, об этом факте упоминается только в [9].

С учетом материала, изложенного в [3], необходимо минимум 3 раунда сети Фейстеля для построения подобных отображений. В работе [5] сформулирована и доказана теорема, связывающая верхнюю границу количества запросов с вероятностью достижения успеха алгоритма-различителя:

$$\left|\Pr[A(f_1, f_2, f_3) = 1] - \Pr[A(f_{2n}) - 1]\right| \le \frac{m^2}{2^n},$$

где f_1, f_2, f_3 – случайные функции из F_n, A – алгоритм-различитель, f_{2n} – случайная функция из F_{2n}, m – количество запросов.

С учетом замечания, упоминающегося в [9], под f_{2n} следует понимать случайную перестановку на множестве I_{2n}.

Рассмотрим подробнее трехраундовую сеть Фейстеля (рис. 1).

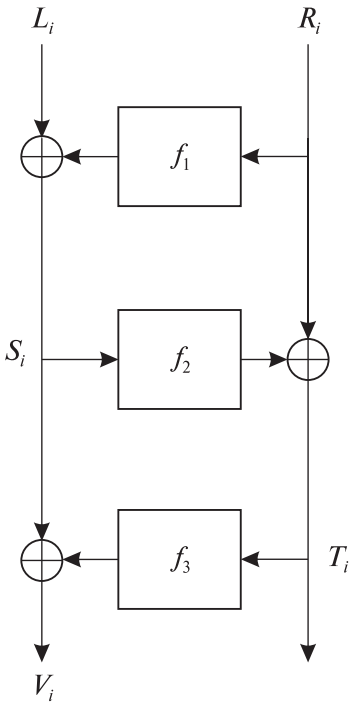

Рис. 1. Трёхраундовая сеть Фейстеля

Более аргументированная атака предложена в [9]. Ее суть состоит в том, что при выполнении равенства (1) фиксируются R_i и R_j, при которых выполнилось равенство (1), а константа L_i переопределяется в L_i'. Проводятся еще два запроса с входящими значениями L_i', R_i и L_i', R_j. В случае выполнения равенства делается заключение о том, что перестановка построена с использованием трехраундовой сети Фейстеля. Рассуждения авторов справедливы для случая, когда произошла коллизия вида $f_1(R_i) = f_1(R_j), i \neq j$. Тогда, изменение входящих данных L_i, R_i и L_i, R_j на L_i', R_i и L_i', R_j также приведет к выполнению равенства (1) в трехраундовой сети Фейстеля. Однако выполнение равенства (1) также возможно и в случае возникновения коллизии вида $f_2(S_i) = f_2(S_j), i \neq j$, что не учитывается авторами. Тогда, изменение входящих данных L_i, R_i и L_i, R_j на L_i', R_i и L_i', R_j не приведет к выполнению равенства (1).

Рассмотрим вероятность выполнения равенства (1) в случайных перестановках. Отметим тот факт, что в работах [3,9,11] неявно подразумевается выполнение условия $L_i = const$.

Сформулируем и докажем лемму 1, определяющую вероятность совпадения левого и правого полублока при использовании случайной перестановки.

Лемма 1. Пусть $T_i, R_i, T_j, R_j, i \neq j$ случайные, независимые и равновероятные элементы множества I_n. Тогда $\Pr[T_i \oplus R_i = T_j \oplus R_j] \leq \frac{1}{2^n}$.

Доказательство. Положим, что

$$T_i \oplus R_i = y, y \in I_n.$$

Представим элемент y в виде $y = y_1, y_2, ..., y_n$, где $y_k \in \{0,1\}; 1 \leq k \leq n$ – значения соответствующих битов. Аналогичным образом представим элементы $T_j = t_{j1}, t_{j2}, ..., t_{jn}; R_j = r_{j1}, r_{j2}, ..., r_{jn}$. Для каждого значения y_k возможны по два соответствующих значения t_{jk}, r_{jk} таких, что

$$t_{jk} \oplus r_{jk} = y_k. \qquad (2).$$

Поскольку элементы T_j, R_j случайные, независимые и равновероятные, t_{jk}, r_{jk} также случайные, независимые и равновероятные. Вероятность того, что t_{jk} и r_{jk} примут одно из необходимых значений для выполнения равенства (2), не превышает величины $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. Аналогично, вероятность того, что t_{jk} и r_{jk} примут второе из соответствующих необходимых значений для выполнения равенства (2), также не превышает величины $\frac{1}{4}$. Вероятность того, что произойдет одно из этих событий, равна сумме вероятностей, $\Pr[t_{jk} \oplus r_{jk} = y_k] \leq \frac{1}{2}$. Применяя аналогичные рассуждения к оставшимся $n-1$ битам, и учитывая независимость каждой пары битов, получим $\Pr[T_i \oplus R_i = T_j \oplus R_j] \leq \frac{1}{2^n}$.

Лемма доказана.

На основании леммы 1 легко сформулировать и доказать теорему, определяющую вероятность совпадения левого и правого полублоков при заданном количестве запросов.

Теорема 1. Пусть $L_i, R_i, 1 < i \leq m$ входящие значения случайной перестановки на множестве I_{2n}, а $V_i, T_i, 1 < i \leq m$ соответствующие им выходящие значения. При проведении серии из m запросов

$$\Pr[T_i \oplus R_i = T_j \oplus R_j] \leq \frac{m^2}{2(2^n - 1)}, 1 < i, j \leq m, i \neq j.$$

Доказательство. При проведении m запросов образуется m пар вида $T_i \oplus R_i, 1 < i \leq m$. Согласно лемме 1, вероятность выполнения равенства $T_i \oplus R_i = T_j \oplus R_j, 1 < i, j \leq m, i \neq j$ между двумя любыми из них не превышает $\frac{1}{2^n}$. Однако, с учетом того, что $L_i = const$, а $R_i \neq R_j, i \neq j$, имеем

$$\Pr[T_i \oplus R_i = T_j \oplus R_j] \leq C_m^2 \cdot \frac{1}{2^n - 1} \leq \frac{m^2}{2(2^n - 1)},$$
$$1 < i, j \leq m, i \neq j$$

Теорема доказана.

Упоминание о теореме 1 встречается в [9], однако, доказательство не приведено.

Очевидно, что для выполнения равенства (1) с вероятностью близкой к 1, количество запросов m должно быть равным $2^{\frac{n}{2}}$. Для атаки, изложенной в [11], рассмотрим вероятность того, что случайная перестановка будет принята за трехраундовую сеть Фейстеля. Согласно теореме 1, вероятность выполнения равенства (1) для случайных перестановок не превышает значения $\frac{m^2}{2(2^n-1)}$. При $m=2^{\frac{n}{2}}$, значение вероятности принимает вид $\frac{2^n}{2(2^n-1)}$. Очевидно, что с увеличением длины блока n, значение вероятности будет стремиться к величине $\frac{1}{2}$. Следовательно, для достаточно больших n, вероятность того, что случайную перестановку примут за трехраундовую сеть Фейстеля, близка к значению $\frac{1}{2}$.

Для атаки, изложенной в [9], рассмотрим вероятность того, что на m запросах не произойдет коллизии $f_1(R_i)=f_1(R_j), i\neq j$ и произойдет коллизия $f_2(S_i)=f_2(S_j), i\neq j$. Поскольку вероятность коллизии $f_1(R_i)=f_1(R_j), i\neq j$ не превышает значения $\frac{1}{2^n}$, имеем

$$\Pr[f_1(R_i)\neq f_1(R_j)]\leq 1-\frac{1}{2^n}, 1<i,j\leq m, i\neq j.$$

Вероятность того, что произойдет коллизия $f_2(S_i)=f_2(S_j), 1<i,j\leq m, i\neq j$, не превышает значения $\frac{1}{2^n}$. Тогда, полная вероятность будет равна произведению вероятностей и не превышает значения $\left(1-\frac{1}{2^n}\right)\frac{1}{2^n}$. Для серии из m запросов вероятность того, что не произойдет коллизии $f_1(R_i)=f_1(R_j), i\neq j$ и произойдет коллизия $f_2(S_i)=f_2(S_j), i\neq j$ между двумя любыми из них, не превышает значения

$$C_m^2\cdot\frac{1}{2^n}\left(1-\frac{1}{2^n}\right)\leq\frac{m^2}{2^{n+1}}\left(1-\frac{1}{2^n}\right).$$

При $m=2^{\frac{n}{2}}$, значение вероятности примет вид $\left(1-\frac{1}{2^n}\right)\frac{2^n}{2^{n+1}}$. Проведя несложные действия, получим $\left(\frac{2^n-1}{2^n}\right)\cdot\frac{1}{2}$. Очевидно, что для достаточно больших значений n, значение первого множителя полученного выражения будет достаточно близким к 1. Следовательно,

$$\Pr[f_1(R_i)\neq f_1(R_j)\wedge f_2(S_i)=f_2(S_j)]\leq\frac{1}{2},$$

$$1<i,j\leq m, i\neq j, m=2^{\frac{n}{2}}.$$

Еще раз напомним, что в этом случае выполняется равенство (1) для $L_i=const$ и не выполняется равенство (1) для $L_i'=const$. Таким образом, с вероятностью, близкой к $\frac{1}{2}$, трехраундовая сеть Фейстеля будет принята за случайную перестановку. С точки зрения безопасности блочных симметричных шифров, такое значение вероятности неразличимости трехраундовой сети Фейстеля достаточно велико. Однако, учитывая тот факт, что авторы атаки рассмотрели не все возможные варианты, не имеет никакого практического значения.

Учитывая изложенное, актуальной является задача нахождения новой атаки на трехраундовую сеть Фейстеля с вероятностью ошибки отличия от случайных перестановок меньшей, чем $\frac{1}{2}$, и приблизительно такой же вычислительной сложностью.

Сформулируем и докажем лемму.

Лемма 2. В трехраундовой сети Фейстеля при количестве запросов m и выполнении условия $R_i=const, 1<i\leq m$, выполняется неравенство $\Pr[T_i=T_j]\leq\frac{m^2}{2^{n+1}}$.

Доказательство. Положим, что при m запросах, $R_i=const, 1<i\leq m$. Поскольку алгоритму-различителю на вход не подаются одинаковые запросы, то $L_i\neq L_j, i\neq j$. Очевидно, что $S_i\neq S_j, i\neq j, 1<i,j\leq m$, поскольку $S_i=f_1(R_i)\oplus L_i$, а все L_i различны. Вероятность коллизии $f_2(S_i)=f_2(S_j)$ не превышает значения $\frac{1}{2^n}$. При проведении m запросов образуется m значений функции f_2 от $S_i, 1<i\leq m$. Следовательно, вероятность коллизии между двумя любыми из них

$$\Pr[f_2(S_i)=f_2(S_j)]\leq C_m^2\cdot\frac{1}{2^n},$$

$$i\neq j, 1<i,j\leq m\Rightarrow\Pr[f_2(S_i)=f_2(S_j)]\leq\frac{m^2}{2^{n+1}}.$$

Лемма доказана.

Следствие из леммы 2:

В трехраундовой сети Фейстеля при проведении m запросов и выполнении условия $R_i=const, 1<i\leq m$, с вероятностью, не превышающей $\frac{m^2}{2^{n+1}}$, одновременно выполняются равенства $T_i=T_j, V_i\oplus L_i=V_j\oplus L_j, i\neq j, 1<i,j\leq m$.

Положим, что критерием различия трехраундовой сети Фейстеля от случайной перестановки является выполнение равенств

$$T_i = T_j, V_i \oplus L_i = V_j \oplus L_j, i \neq j, 1 < i, j \leq m .$$

Очевидно, что выполнение этих равенств потенциально возможно и для случайной перестановки (с малой вероятностью), что приведет к ошибке алгоритма-различителя. Оценим вероятность такого события.

Теорема 2. При проведении m запросов и выполнении условия $R_i = const, 1 < i \leq m$, вероятность того, что случайную перестановку примут за трехраундовую сеть Фейстеля, не превышает значения $\frac{m^2}{2^{n+1}(2^n - 1)}$.

Доказательство. Для случайных перестановок вероятность выполнения равенства $V_i \oplus L_i = V_j \oplus L_j, i \neq j$ не превышает значения $\frac{1}{2^n - 1}$, вероятность выполнения равенства $T_i = T_j, i \neq j$ не превышает значения $\frac{1}{2^n}$. Поскольку события являются независимыми, то полная вероятность того, что произойдут оба события, не превышает произведения вероятностей $\Pr[V_i \oplus L_i = V_j \oplus L_j \wedge T_i = T_j] \leq \frac{1}{2^n(2^n - 1)}, i \neq j$. Тогда, вероятность того, что равенства выполнятся между любыми двумя запросами, не превышает значения

$$\Pr[V_i \oplus L_i = V_j \oplus L_j \wedge T_i = T_j] \leq$$

$$\leq C_m^2 \cdot \frac{1}{2^n(2^n - 1)} \leq \frac{m^2}{2^{n+1}(2^n - 1)}, i \neq j.$$

Теорема доказана.

Очевидно, что при таком критерии различия, для того, чтобы выполнились оба равенства с вероятностью близкой к 1, количество запросов m должно быть равным $2^{\frac{n}{2}}\sqrt{2}$. Тогда, значение вероятности ошибки примет вид $\frac{1}{2^n - 1}$. При достаточно больших значениях n, вероятность ошибки будет стремиться к 0.

Следует особо отметить тот факт, что рассматривались атаки на основе выбранных открытых текстов. В [3] показано, что трехраундовая сеть Фейстеля отличима от случайных перестановок на множестве I_{2n} с вероятностью близкой к 1, при условии, что алгоритму различителю доступны обратные запросы, то есть атака на основе выбранных шифртекстов.

ВЫВОДЫ

В статье рассмотрены основные атаки на трехраундовую сеть Фейстеля с целью определения отличия такой сети от случайной перестановки на множестве I_{2n}, проанализированы критерии, на основании которых проводится различие. С учетом того, что эти критерии представляют собой выполнения определенных равенств, рассмотрены вероятности выполнения этих равенств в случайных перестановках на множестве I_{2n}. На основании полученных результатов можно сделать следующие выводы:

• при проведении серии из m запросов для атаки, изложенной в [3], вероятность того, что случайная перестановка будет принята за 3-раундовую сеть Фейстеля, близка к значению $\frac{1}{2}$;

• для атаки, изложенной в [9], при проведении серии из m запросов вероятность того, что 3-раундовая сеть Фейстеля будет принята за случайную перестановку, близка к значению $\frac{1}{2}$.

Учитывая, что вероятность ошибки в различии 3-раундовой сети Фейстеля от случайных перестановок на множестве I_{2n} близка к значению $\frac{1}{2}$, авторами предложена новая атака и новые критерии, на основании которых проводится различие. По сравнению с результатами, приведенными в [3,9], вычислительная мощность предложенной атаки выросла в $\sqrt{2}$ раза, а вероятность ошибки близка к 0. Учитывая, что основные результаты работ [3, 9] были получены в 90-х годах прошлого столетия, возрастание вычислительной мощности предложенной атаки является несущественным. Более того, предложенная атака и критерии различия 3-раундовой сети Фейстеля от случайных перестановок на множестве I_{2n} позволяют безошибочно, с вероятностью близкой к 1, на основании серии из $2^{\frac{n}{2}}\sqrt{2}$ запросов отличить 3-раундовый блочный симметричный шифр на основе сети Фейстеля от случайной перестановки.

Литература.

[1] *Josef Pieprzyk*. How to Construct Pseudorandom Permutations from Single Pseudorandom Functions. Advances in Cryptology EuroCrypt ‘90.

[2] *Mihir Bellare, Phillip Rogaway*. Introduction to Modern Cryptography.

[3] *M. Luby and C. Rackoff*. How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput, Vol. 17, No. 2, April 1988.

[4] *Ueli M. Maurer*. A simplified and Generalized Treatment of Luby – Rackoff Pseudorandom Permutations Generator. Advances in Cryptology EuroCrypt ‘92.

[5] *Gilles-Francois Piret*. Block Ciphers: Security Proofs, Cryptanalysis, Design, and Fault Attacks. Universite Catholique de Louvain Faculte des Sciences Appliquees Laboratoire de Microelectronique UCL Crypto Group, Janvier 2005.

[6] *Zulfikar Amin Ramzan*. A Study of Luby – Rackoff Ciphers. Massachusetts institute of technology, January 2001.

[7] *Moni Naor, Omer Reingold.* On the Construction of Pseudo – Random Permutations: Luby – Rackoff Revisited. Electronic Colloquium on Computational Complexity Report TR97-005.

[8] Shafi Goldwasser, Mihir Bellare. Lecture Notes on Cryptography. Cambridge, Massachusetts, August 2001.

[9] William Aiello, Ramarathnam Venkatesan. Foiling Birthday Attacks in Length – Doubling Transformations. Advances in Cryptology EuroCrypt '96

[10] Jacques Patarin. New Results on Pseudorandom Permutation Generators Based on the DES Scheme. Advances in Cryptology Crypto '91.

[11] Jacques Patarin. Generic Attacks on Feistel Schemes. AsiaCrypt 2001.

Поступила в редколлегию 14.09.2009

Бондаренко Михаил Федорович, член-корреспондент НАН Украины, Лауреат государственной премии Украины, доктор технических наук, профессор, ректор Харьковского национального университета радиоэлектроники.

Небывайлов Алексей Борисович, аспирант кафедры БИТ ХНУРЭ, главный консультант управления спецтелекоммуникаций и технического обеспечения Государственного управления делами Президента Украины. Область научных интересов: блочные шифры, криптоанализ.