Досліджена SPN-структура (substitution-permutation network) блокового симетричного шифру. Висунутий критерій оцінки її ефективності основою якого є можливість розрізнення такої структури та випадкової перестановки. Висунута та доведена теорема про максимальну вірогідність розрізнення SPN-структури та випадкової перестановки. Для 2-х циклової модифікації такої структури знайдено алгоритм-розрізнювач від випадкової перестановки

Ключові слова: блоковий симетричній шифр, високорівнева конструкція, SPN-структура, випадкова перестановка, алгоритм-розрізнювач

Исследована SPN-структура (substitution-permutation network) блочного симметричного шифра. Выдвинут критерий оценки ее эффективности, основой которого является возможность отличения такой структуры от случайной перестановки. Выдвинута и доказана теорема про максимальную вероятность отличения SPN-структуры и случайной перестановки. Для 2-х цикловой модификации такой структуры найден алгоритм-различитель от случайной перестановки

Ключевые слова: блочный симметричный шифр, высокоуровневая конструкция, SPN-структура, случайная перестановка

УДК 681.3.06
DOI: 10.15587/1729-4061.2014.30988

ОЦЕНКА ЭФФЕКТИВНОСТИ SPN-СТРУКТУРЫ БЛОЧНОГО СИММЕТРИЧНОГО ШИФРА

Д. С. Кайдалов
Аспирант*
E-mail: dmtr.kd@gmail.com
Р. В. Олейников
Доктор технических наук, профессор*
E-mail: roliynykov@gmail.com
*Кафедра безопасности информационных технологий
Харьковский национальный университет радиоэлектроники
пр. Ленина 14, г. Харьков, Украина, 61166

1. Введение

Опыт проведения открытых криптографических конкурсов показал, что в настоящее время при проектировании симметричных блочных шифров основное внимание уделяется раундовому преобразованию, обоснованию его дифференциальных, линейных и алгебраических свойств, а также схеме формирования раундовых подключей. Выбор высокоуровневой конструкции шифра осуществляется на основе предпочтений разработчика и в подавляющем большинстве случаев не имеет теоретического обоснования.

Тем не менее, при разработке алгоритма целесообразно опираться на некоторую численную оценку эффективности. С точки зрения обеспечения требуемых криптографических свойств и стойкости здесь целесообразно использовать модель блочного шифра как случайной перестановки, а с точки зрения программной (или аппаратной) реализации – требуемое количество операций.

Эффективность высокоуровневой конструкции блочного шифра целесообразно оценивать через сложность различения перестановки, сформированной этой структурой (при использовании одного ключа шифрования), от случайной соответствующей степени, поскольку именно множество случайных перестановок степени является моделью идеального блочного шифра [1]. Сложность выполнения алгоритма-различителя и достигаемая вероятность успеха являются численными показателями эффективности высокоуровневой конструкции. Для исключения влияния свойств конкретной раундовой функции необходимо использовать идеализированное раундовое преобразование, такое как случайная функция или случайная перестановка.

В качестве критерия эффективности высокоуровневой конструкции блочного симметричного шифра целесообразно использовать возможность различения случайной перестановки и подстановки, сформированной шифрующем преобразованием [2], а в качестве показателей эффективности – вероятность успешного различения и сложность работы соответствующего алгоритма-различителя [3].

Наряду с цепью Фейстеля с схемой Лей-Месси, SPN-структура (substitution-permutation network) является одной из наиболее распространенных высокоуровневых конструкций блочных симметричных шифров. В частности, это преобразование использовано в наиболее широко распространенном во всем мире алгоритме AES/Rijndael, шифрах Anubis, GrandCru, Noekeon, «Калина» и др. Исследования эффективности различения цепи Фейстеля и схемы Лей-Месси были рассмотрены авторами в [4] и [5] соответственно. В данной статье проводится анализ SPN-структуры.

2. Обзор существующих публикаций и постановка проблемы

Одной из основополагающих работ по оценке эффективность некоторой конструкции путем сравнения ее со случайной перестановкой является работа M. Luby и C. Rackoff [2]. Авторы публикации исследовали цепь Фейстеля, которая является основой алгоритма DES.

Данная работа дала толчок к появлению других публикаций на эту тему. К примеру, U. M. Maurer в своей работе [3] развивает и улучшает результаты исследований M. Luby и C. Rackoff. J. Patarin применил данный метод к алгоритму DES с различным количеством раундов [6]. В [7] он оценил возможность атаковать 5 раундов, а [8] оценивается 6 и более раундов алгоритма DES. Авторы текущей статьи также провели ряд исследований по цепи Фейстели и смогли получить еще более точные оценки для данной конструкции [4].

Основываясь на этих работах, S. Vaudenay в [9] провел анализ схемы Лей-Месси, показав, что метод, предложенный M. Luby и C. Rackoff, применим не только для цепи Фейстеля. В свою очередь, авторы текущей статьи также проводили исследования схемы Лей-Месси и разработали несколько новых алгоритмов-различителей, опубликованных в [5].

Однако совсем мало работ, в которых осуществляются попытки применить такой подход к SPN-структуре. Во многом это продиктовано большими различиями между цепью Фейстеля и схемой Лей-Месси с одной стороны и SPN-структурой с другой. Несмотря на это, авторы поставили перед собой цель оценить эффективность SPN-структуры путем сравнения ее со случайной перестановкой (как это было сделано в [4] и [5] для других конструкций), чтобы в конечном итоге получить сравнительную оценку всех трех структур.

3. Цель и задачи исследования

Целью проводимых исследований являлось получение количественных оценок, по которым можно было бы оценить эффективность SPN-структуры и сравнить ее с другими высокоуровневыми конструкциями блочных шифров. Как уже было упомянуто выше, такими оценками являются вероятности различения SPN-структуры и случайной перестановки.

Для достижения поставленной цели решались следующие задачи:

– определение максимально достижимой вероятности различения SPN-структуры и случайной перестановки. Требовалось вывести выражение, которое позволит рассчитать такую характеристику и доказать его математически.

– нахождение алгоритма-различителя для 2-х раундовой SPN-структуры. Расчет вероятности, с которой такой алгоритм позволяет отличать от случайной перестановки.

– нахождение алгоритма-различителя для 3-х и более раундов SPN-структуры. Обоснование неотличимости 3-х и более раундов от случайной перестановки.

4. Модель алгоритма-различителя

В этом, а также последующих разделах, будут использоваться следующие условные обозначения:

I_n – множество битовых векторов длины n;

I_{2n} – множество битовых векторов длины 2n;

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

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

σ_n – множество перестановок степени n;

σ_{2n} – множество перестановок степени 2n;

ψ – биективное отображение на основе цепи Фейстеля;

ς – биективное отображение на основе схемы Лей-Месси;

ϑ – биективное отображение на основе SPN-структуры;

η_i – i-й алгоритм-различитель высокоуровневой структуры блочного шифра и случайной перестановки;

η_* – лучший теоретический алгоритм-различитель (возможно, гипотетический) высокоуровневой структуры блочного шифра и случайной перестановки; используется для оценки верхней границы эффективности различения;

P_1 – вероятность, с которой алгоритм-различитель определяет высокоуровневую структуру блочного шифра;

P_1^* – вероятность, с которой алгоритм-различитель определяет случайную функцию (перестановку);

$x \bullet y$ – конкатенация двух векторов x и y.

Алгоритм-различитель (distinguisher) η_i предназначен для определения преобразования, которое было использовано для формирования выходной последовательности по входной (блочный шифр или случайная перестановка) [3].

Метод различения основан на поиске специфических признаков, характерных для блочного шифра. Сложность различения может определяться как для конкретного алгоритма, так и как верхняя граница для произвольного (любого возможного) алгоритма.

Алгоритм (рис. 1) получает на входе множество открытых текстов $\{(x_i), 1 \le i \le m\}$ и множество соответствующих шифрованных текстов $\{(y_i), 1 \le i \le m\}$. После завершения работы на выходе алгоритма формируется значение «1» (использована высокоуровневая конструкция блочного шифра) либо «0» (выходные данные сформированы случайной перестановкой или функцией).

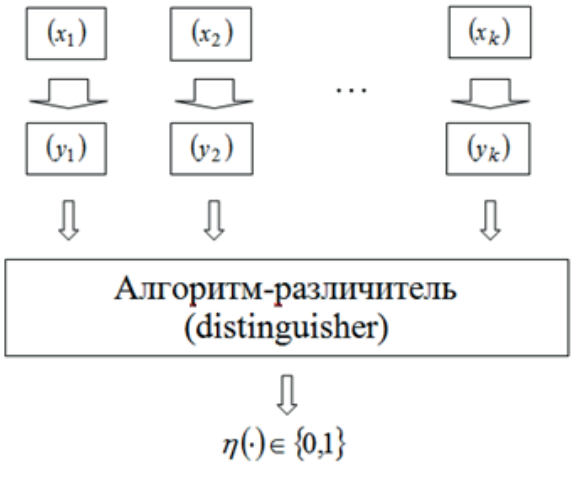

Рис. 1. Модель алгоритма-различителя

Поскольку в качестве раундового преобразования в модели блочного шифра используется случайная перестановка или случайная функция, то появление

специфических признаков тоже является случайным событием, имеющим некоторую вероятность (по которой определяется вероятность успешного различения и эффективность конкретного алгоритма). В то же время, при выборе случайной перестановки существует ненулевая вероятность того, что такая перестановка будет иметь признаки, характерные для блочного шифра, и алгоритм-различитель примет неверное решение. Модуль разности этих вероятностей и определяет эффективность конкретного алгоритма-различителя:

$$\mathrm{Adv}_{\eta_i}(\nu,\sigma_{2n}) = \left|P_1 - P_1^*\right|, \quad (1)$$

где $\nu \in \{\psi, \varsigma, \vartheta\}$ – некоторая высокоуровневая структура блочного шифра.

Таким образом, различение является вероятностным и допускает появление ошибок первого рода (последовательности, сформированные блочным шифром, принимаются сформированными случайной перестановкой из-за отсутствия характерных признаков) и второго рода (последовательности, сформированные случайной перестановкой, имеют специфические признаки, по которым принимается решение об использовании блочного шифра).

Отметим, что алгоритм-различитель η_i может быть представлен как некоторая машина Тьюринга, так и как отображение $\eta_i : \left(\{0,1\}^{2n}\right)^k \to \{0,1\}$, не требующее дополнительной памяти.

5. Модель SPN-структуры

В соответствии с принципами Шеннона [10], SPN-структура чередует операции перемешивания (diffusion) и рассеивания (confusion), реализуемые с помощью линейных и нелинейных преобразований соответственно.

В отличие от цепи Фейстеля и схемы Лей-Месси, для реализации корректного расшифрования в раундовом преобразовании SPN-структур требуется применение исключительно биективных отображений (перестановок), т. е. SPN-структура не может быть построена на основе случайных функций.

По аналогии с представлением внутреннего состояния алгоритмов Square и AES/Rijndael, обрабатываемый шифром блок целесообразно представить в виде прямоугольной матрицы размером $n_c \times n_b$ элементов, каждый из которых имеет размер n_e битов, причем размер блока равен $2n = n_c \times n_b \times n_e$ битов. Для обеспечения требуемых криптографических свойств и эффективности программной реализации целесообразно выбирать $n_c = n_b \cdot 2l, l \in \{1,2,...\}$. Кроме того, все современные шифры являются байт-ориентированными, поэтому для AES/Rijndael, «Калина» и других алгоритмов $n_e = 8$.

Как и в случае с предыдущими высокоуровневыми конструкциями, для исключения влияния конкретных компонентов принимается, что в раундовом преобразовании SPN-структуры используются случайные перестановки. Проводя аналогию с AES/Rijndael, такую случайную перестановку можно назвать Super-S-box (см., например, [11]).

Таким образом, рассматриваемая модель шифрующего преобразования SPN-структуры состоит из итеративного применения слоя случайных перестановок и обмена элементов между колонками матрицы состояния.

Один цикл шифрования алгоритмом на основе SPN-структуры при $n_c = n_b$ представлен на рис. 2.

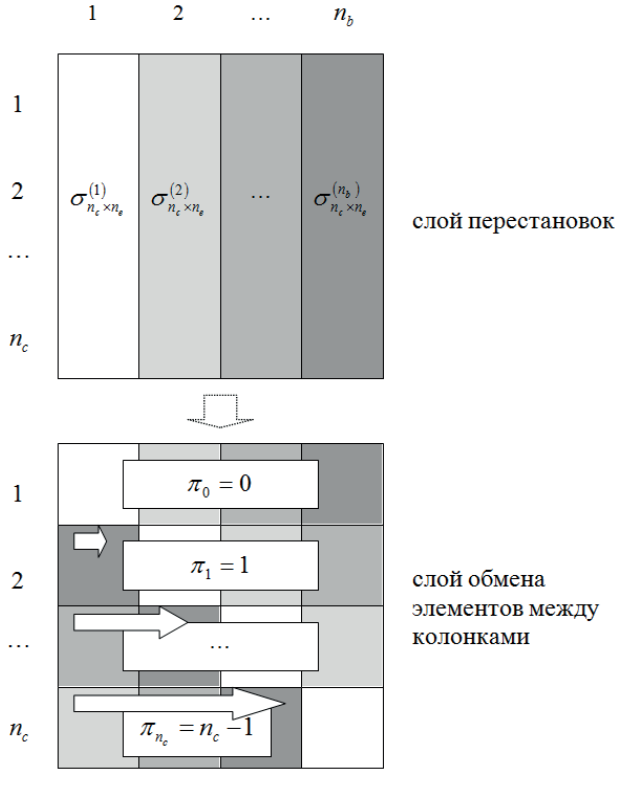

Рис. 2. Цикл шифрования алгоритмом на основе SPN-структуры

В общем случае, модель s-циклового шифра на основе SPN-структуры может быть представлен в виде формулы

$$\vartheta = \prod_{i=1}^{s}\left(\pi_0 \bullet \pi_1 \bullet ... \bullet \pi_{n_c}\right) \circ \left(\sigma^{(1,i)}_{n_c \times n_e} \bullet \sigma^{(2,i)}_{n_c \times n_e} \bullet ... \bullet \sigma^{(n_b,i)}_{n_c \times n_e}\right). \quad (2)$$

На вход шифрующего преобразования подается значение $x_i = \left(x_i^{(1)} \bullet x_i^{(2)} \bullet ... \bullet x_i^{(n_b)}\right)$, на выходе формируется $y_i = \left(y_i^{(1)} \bullet y_i^{(2)} \bullet ... \bullet y_i^{(n_b)}\right)$.

В теореме 1 рассматривается модель шифрующего преобразования на основе SPN-структуры с двумя циклами шифрования.

6. Максимальная вероятность различения 2-цикловой SPN-структуры

Теорема 1 (верхняя граница различения 2-цикловой SPN-структуры и случайной перестановки на ограниченном числе запросов).

Максимальная вероятность различения случайной перестановки σ_{2n} и 2-цикловой SPN-структуры с

размером блока $2n$ битов и внутренним состоянием, представляемым в виде матрицы размером $n_c \times n_b$ элементов, каждый из которых имеет размер n_e битов ($2n = n_c \times n_b \times n_e$), при соответствии соотношений размеров матрицы условию $n_c = n_b \cdot 2l, l \in \{1,2,...\}$, применении случайных перестановок $\sigma_{\frac{2n}{n_c \cdot n_e}}$ в раундовом преобразовании, для k запросов $\left(2 \le k \le 2^{\frac{n_c \cdot n_e}{n_b}}\right)$ на входе алгоритма-различителя не превышает значения

$$\mathrm{Adv}_{\eta^*}(\vartheta, \sigma_{2n}) =$$
$$= \left| P_1\left(\eta_*(f(x_1),...,f(x_k)) = 1 : f \in_R \vartheta^{(2)}\right) - P_1^*\left(\eta_*(f(x_1),...,f(x_k)) = 1 : f \in_R \sigma_{2n}\right)\right| \le$$
$$\le \left| 1 - \prod_{i=0}^{k-2}\left(1 - 2^{-i\frac{n_c \cdot n_e}{n_b}}\right)^{(n_b-1)(k-i-1)} - \prod_{i=0}^{\frac{k(k-1)}{2}-1} \frac{\left(2^{\frac{n_c \cdot n_e}{n_b}} - 1\right)^{n_b} - i}{\left(2^{n_c \cdot n_e} - i\right)} \right| \approx$$
$$\approx \left| 1 - \left(1 - 2^{-\frac{n_c \cdot n_e}{n_b}}\right)^{\frac{k(k-1)(n_b-1)}{2}} - 2^{-\frac{n_c \cdot n_e \cdot k(k-1)}{2}} \cdot \left(2^{\frac{n_c \cdot n_e}{n_b}} - 1\right)^{\frac{n_b k(k-1)}{2}} \right|.$$

Доказательство.

Вероятность различения SPN-структуры оценивается следующим образом.

Для запроса из одной пары элементов (x_i, x_j), $1 \le i < j \le k$, при отличающемся входе только для одной случайной перестановки (активный Super-S-box), на следующем цикле на каждую перестановку поступит $\frac{n_c}{n_b}$ элементов с активизированной. Коллизионные значения, необходимые для различения, могут отсутствовать или появиться на входе от одной до $(n_b - 1)$ перестановок (коллизии по всем элементам возможны только для случайной функции, но не перестановки).

Соответственно, вероятность появления коллизии на входе одной перестановки равна $p_\sigma = 2^{-\frac{n_c \cdot n_e}{n_b}}$, а появления хотя бы одной коллизии на входе всех подстановок второго раунда вычисляется как

$$p_2 = 1 - \left(1 - 2^{-\frac{n_c \cdot n_e}{n_b}}\right)^{n_b - 1}. \quad (4)$$

Выражение (4) определяет вероятность различения SPN-структуры и случайной перестановки на одной паре запросов.

Для запроса, состоящего из k входных значений, можно составить $C_k^2 = \frac{k(k-1)}{2}$ различных пар. Вероятность появления коллизии среди промежуточных значений на входе случайных подстановок для всех пар равна

$$p_{\eta_*} = 1 - \left(\left(1 - \frac{1}{2^{\frac{n_c \cdot n_e}{n_b}}}\right)^{n_b - 1}\right)^{k-1} \left(\left(1 - \frac{1}{2^{\frac{n_c \cdot n_e}{n_b}} - 1}\right)^{n_b - 1}\right)^{k-2} ...$$
$$... \left(\left(1 - \frac{1}{2^{\frac{n_c \cdot n_e}{n_b}} - (k-2)}\right)^{n_b - 1}\right)^{k-(k-1)} =$$
$$= 1 - \prod_{i=0}^{k-2}\left(1 - \frac{1}{2^{\frac{n_c \cdot n_e}{n_b}} - i}\right)^{(n_b-1)(k-i-1)}.$$

При малом размере выборки $\left(\#\{x_i\} << 2^{\frac{n_c \cdot n_e}{n_b}}\right)$ вероятность появления коллизии на входе случайной перестановки второго цикла изменяется незначительно, откуда можно воспользоваться аппроксимацией

$$p_{\eta_*} \approx 1 - \left(1 - \frac{1}{2^{\frac{n_c \cdot n_e}{n_b}}}\right)^{\frac{k(k-1)(n_b-1)}{2}}. \quad (5)$$

Вероятность появления повторяющихся значений на выходе блоков, соответствующих границе Super-S-box, для случайной перестановки σ_{2n} можно оценить следующим образом.

Число комбинаций для одной пары, при которых выходные значения не повторяются ни в одном из блоков, равно $p_1 = 2^{-n_c \cdot n_e} \cdot \left(2^{\frac{n_c \cdot n_e}{n_b}} - 1\right)^{n_b}$. Для запроса, состоящего из k значений, можно составить $C_k^2 = \frac{k(k-1)}{2}$ пар, и вероятность того, что значения не повторятся ни в одной паре, равна

$$P_1^*\left(\eta_*(f(x_1),...,f(x_k)) = 1 : f \in_R \sigma_{2n}\right) =$$
$$= \frac{\left(2^{\frac{n_c \cdot n_e}{n_b}} - 1\right)^{n_b} \cdot \left(\left(2^{\frac{n_c \cdot n_e}{n_b}} - 1\right)^{n_b} - 1\right) \cdot ... \cdot \left(\left(2^{\frac{n_c \cdot n_e}{n_b}} - 1\right)^{n_b} - \frac{k(k-1)}{2} + 1\right)}{2^{n_c \cdot n_e} \cdot \left(2^{n_c \cdot n_e} - 1\right) \cdot ... \cdot \left(2^{n_c \cdot n_e} - \frac{k(k-1)}{2} + 1\right)} =$$
$$= \prod_{i=0}^{\frac{k(k-1)}{2}-1} \frac{\left(2^{\frac{n_c \cdot n_e}{n_b}} - 1\right)^{n_b} - i}{\left(2^{n_c \cdot n_e} - i\right)}.$$

При малом размере выборки $\left(\#\{x_i\} << 2^{\frac{n_c \cdot n_e}{n_b}}\right)$ вероятность появления коллизии на входе блоков, соответствующих границе Super-S-box, изменяется незначительно, откуда можно воспользоваться аппроксимацией

$$P_1^*\left(\eta_*(f(x_1),...,f(x_k))=1 : f \in_R \sigma_{2n}\right) \approx$$
$$\approx 2^{-\frac{n_c \cdot n_e \cdot k \cdot (k-1)}{2}} \cdot \left(2^{\frac{n_c \cdot n_e}{n_b}} - 1\right)^{\frac{n_b k(k-1)}{2}}.$$

Теорема доказана.

7. Алгоритм-различитель для 2-цикловой SPN-структуры

Для k входных аргументов $\left(2 \le k \le 2^{\frac{n_c \cdot n_e}{n_b}} + 1\right)$, выполняющих активизацию одной перестановки:

$$x_i^{(t)} \ne x_j^{(t)}, x_i^{(l)} = x_j^{(l)}, 1 \le l \le n_b, l \ne t, t = \text{const},$$

$$x_i = \left(x_i^{(1)} \bullet x_i^{(2)} \bullet ... \bullet x_i^{(n_b)}\right), \; x_j = \left(x_j^{(1)} \bullet x_j^{(2)} \bullet ... \bullet x_j^{(n_b)}\right),$$

$1 \le i < j \le k$ проверяется наличие коллизий на выходе каждой перестановки второго цикла: $y_i^{(l)} = y_j^{(l)}, 1 \le l \le n_b$, $1 \le i < j \le k$.

В случае выполнения равенства хотя бы для одного аргумента возвращаемое значение будет «1» (обнаружена SPN-структура), иначе «0».

Утверждение (сложность работы алгоритма-различителя).

2-цикловая SPN-структура с размером блока $2n$ битов и внутренним состоянием, представляемым в виде матрицы размером $n_c \times n_b$ элементов, каждый из которых имеет размер n_e битов ($2n = n_c \times n_b \times n_e$), при соответствии соотношений размеров матрицы условию $n_c = n_b \cdot 2l, l \in \{1,2,...\}$, применении случайных перестановок $\sigma_{\frac{2n}{n_c \cdot n_e}}$ в раундовом преобразовании, будет определена алгоритма-различителем не более чем за $2^{\frac{n_c \cdot n_e}{n_b}} + 1$ запросов.

Доказательство следует из теоремы 1.

График зависимости верхней границы вероятности различения 2-цикловой SPN-структуры с параметрами $n_c = 4, n_b = 4, n_e = 8$ (шифр, эквивалентный 2-цикловому AES на случайных перестановках Super-S-box) от количества запросов, приведен на рис. 3.

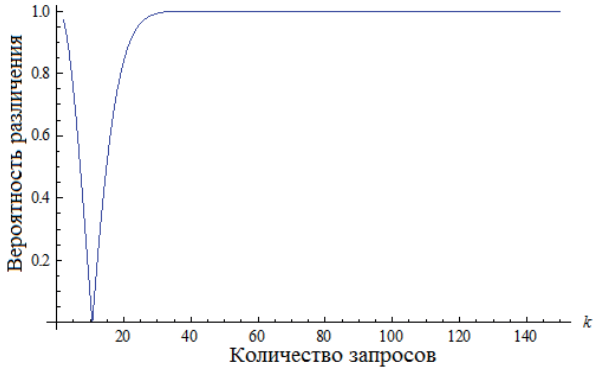

Рис. 3. График зависимости верхней границы вероятности различения 2-цикловой SPN-структуры от количества запросов

В этом случае существует определенное количество запросов, при котором преимущество различения становится равным нулю. При уменьшении числа запросов резко возрастает вероятность определения случайной перестановки (второе слагаемое суммы под модулем в (3), рис. 4), при увеличении количества аргументов алгоритма-различителя увеличивается вероятность определения SPN-структуры (первое слагаемое суммы под модулем в (3), рис. 5), которая становится равной 1 после порогового значения (см. утверждение 1).

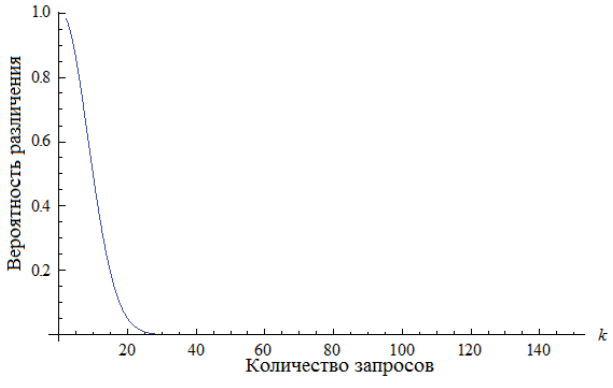

Рис. 4. График зависимости верхней границы вероятности определения случайной перестановки алгоритмом-различителем 2-цикловой SPN-структуры от количества запросов

Как видно из графиков на рис. 3–5, различение даже 2-цикловой SPN-структуры является сложной задачей. Значение, возвращаемое алгоритмом-различителем, в значительной степени зависит не только от типа исследуемого преобразования (блочный шифр или случайная перестановка), но и от количества поданных запросов.

Если для других высокоуровневых структур блочных шифров существует оптимальное количество запросов или некоторый предел, максимизирующий преимущество, то для 2-цикловой SPN-структуры такого значения не существует. Можно определить только пороговое значение, при котором алгоритм-различитель с равной вероятностью будет определять как SPN-структуру, так и случайную перестановку. При меньшем числе запросов предпочтение будет отдаваться случайной перестановке, при большем – SPN-структуре.

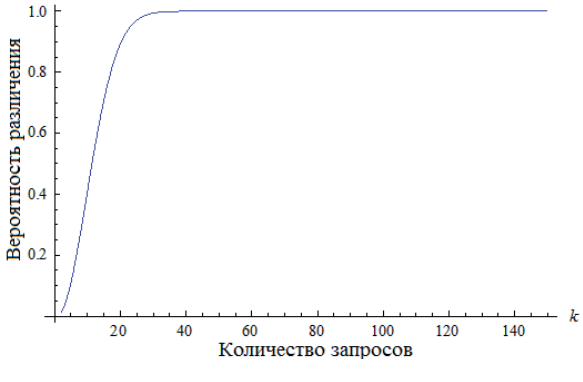

Рис. 5. График зависимости верхней границы вероятности различения 2-цикловой SPN-структуры алгоритмом-различителем от количества запросов

8. Различение 3-цикловой SPN-структуры

Как и для 2-циклового преобразования, в соответствии с для $s=3$ на вход SPN-структуры подается открытый текст $x_i=\left(x_i^{(1)}\bullet x_i^{(2)}\bullet\ldots\bullet x_i^{(n_b)}\right)$, на выходе формируется шифртекст $y_i=\left(y_i^{(1)}\bullet y_i^{(2)}\bullet\ldots\bullet y_i^{(n_b)}\right)$. В отличие от предыдущего случая, для обнаружения коллизии на выходе необходимо появление совпадающих значений, как на выходе первого цикла, так и на выходе второго.

Теорема 2 (эффективность различения 3-цикловой SPN-структуры и случайной перестановки).

Преимущество произвольного алгоритма-различителя случайной перестановки σ_{2n} и 3-цикловой SPN-структуры с размером блока $2n$ битов и внутренним состоянием, представляемым в виде матрицы размером $n_c\times n_b$ элементов, каждый из которых имеет размер n_e битов ($2n=n_c\times n_b\times n_e$), при соответствии соотношений размеров матрицы условию $n_c=n_b\cdot 2l, l\in\{1,2,...\}$, применении случайных перестановок $\sigma_{\frac{2n}{n_c\cdot n_e}}$ в раундовом преобразовании, для произвольного количества запросов равно нулю:

$$\mathrm{Adv}_{\eta^*}(\vartheta,\sigma_{2n})=$$
$$=\left|P_1\left(\eta_*(f(x_1),...,f(x_k))=1:f\in_R\vartheta^{(3)}\right)-P_1^*\left(\eta_*(f(x_1),...,f(x_k))=1:f\in_R\sigma_{2n}\right)\right|=0. \quad (6)$$

Доказательство.

Для появления совпадающих значений на выходе SPN-преобразования необходимо, чтобы на входе, по крайней мере, одной подстановки последнего цикла были только коллизионные значения, т.е. требуется не менее n_c одинаковых элементов ($2^{n_c\cdot n_e}$ бит) после 2-го цикла.

Оптимальная активизация подразумевает подачу разных значений на вход одной перестановки и одинаковые значения на все остальные перестановки первого цикла. Только в этом случае можно добиться максимального количества одинаковых элементов на входе второго цикла, соответственно, максимальной вероятности появления коллизионных значений на выходе.

Для запроса из двух элементов $\left(x_i,x_j\right), 1\le i<j\le k$ совпадающие значения (при оптимальной активизации входных значений) появятся только при возникновении коллизии в одном из следующих случаев:

– один совпадающий элемент после 2-го цикла, $\left(n_c-1\right)$ элементов после 1-го цикла;

– два совпадающих элемента после 2-го цикла, $\left(n_c-2\right)$ элементов после 1-го цикла;

– ...

– $\left(n_c-1\right)$ совпадающих элементов после 2-го цикла, один элемент после 1-го цикла.

Одновременное появление n_c одинаковых элементов во внутреннем состоянии после первого или второго цикла при оптимальной стратегии невозможно, но такое событие имеет ненулевую вероятность при случайных значениях на входе SPN-преобразования, активизирующих не менее двух перестановок первого цикла.

Таким образом, для различения 3-цикловой SPN-структуры нужно одновременное появление не менее n_c коллизионных элементов в промежуточных состояниях (после первого и второго цикла).

Вероятность появления такого количества одинаковых элементов равна $\left(2^{-\frac{n_c\cdot n_e}{n_b}}\right)^{n_c}=2^{-\frac{n_c^2\cdot n_e}{n_b}}$.

Соответственно, для k запросов вероятность одновременного появления n_c коллизионных элементов хотя бы в одном из них равна

$$P_1\left(\eta_*(f(x_1),...,f(x_k))=1:f\in_R\vartheta^{(3)}\right)=1-\left(1-2^{-\frac{n_c^2\cdot n_e}{n_b}}\right)^{\frac{k(k-1)}{2}}. \quad (7)$$

Для случайной перестановки степени $2n$ вероятность появления совпадающих n_c элементов на выходе $P_1^*\left(\eta_*(f(x_1),...,f(x_k))=1:f\in_R\sigma_{2n}\right)$ определяется следующим образом.

Каждый элемент содержит $\frac{n_c}{n_b}\cdot n_e$ битов, и для n_c элементов вероятность совпадения равна $\left(2^{-\frac{n_c\cdot n_e}{n_b}}\right)^{n_c}=2^{-\frac{n_c^2\cdot n_e}{n_b}}$.

Аналогично, для k запросов можно сформировать $C_k^2=\frac{k(k-1)}{2}$ пар, и вероятность одновременного появления n_c коллизионных элементов хотя бы в одной из них равна

$$P_1^*\left(\eta_*(f(x_1),...,f(x_k))=1:f\in_R\sigma_{2n}\right)=1-\left(1-2^{-\frac{n_c^2\cdot n_e}{n_b}}\right)^{\frac{k(k-1)}{2}}. \quad (8)$$

Преимущество произвольного алгоритма-различителя (использующего как оптимальную активизацию, так и случайные запросы), равна модулю разности (7) и (8):

$$\mathrm{Adv}_{\eta^*}(\vartheta,\sigma_{2n})=$$
$$=\left|P_1\left(\eta_*(f(x_1),...,f(x_k))=1:f\in_R\vartheta^{(3)}\right)-P_1^*\left(\eta_*(f(x_1),...,f(x_k))=1:f\in_R\sigma_{2n}\right)\right|=$$
$$=\left|1-\left(1-2^{-\frac{n_c^2\cdot n_e}{n_b}}\right)^{\frac{k(k-1)}{2}}-1+\left(1-2^{-\frac{n_c^2\cdot n_e}{n_b}}\right)^{\frac{k(k-1)}{2}}\right|=0.$$

Доказательство окончено.

Следствие (неразличимость 3-цикловой SPN-структуры и случайной перестановки).

Не существует эффективного алгоритма-различителя для 3-цикловой SPN-структуры и случайной перестановки. Выходные значения любого такого алгоритма являются некоторой случайной величиной, не зависящей от типа анализируемого преобразования.

9. Выводы

В ходе исследований были получены количественные оценки эффективности SPN-структуры основанные на вероятности ее отличения от случайной перестановки. Данный подход уже был применен к цепи Фейстеля и схеме Лей-Месси, поэтому целесообразно было сделать аналогичное исследование для SPN-структуры.

Для этого в первую очередь была найдена максимально возможная вероятность различения SPN-структуры и случайной перестановки. Была выдвинута и доказана теорема описывающая математическое выражения для получения такой вероятности.

Также проводились исследования по поиску конкретных алгоритмов-различителей для различного числа раундов. В результате был найден алгоритм-различитель для 2-х раундовой SPN-структуры. Для 3-х и более раундов было доказано, что построение такого алгоритма невозможно.

В целом результаты исследований могут свидетельствовать о высокой эффективности SPN-структуры от атак подобного рода, основанных на поиске отличий от случайной перестановки.

В дальнейшем полученные результаты могут быть использованы для сравнения с другими высокоуровневыми конструкциями блочных симметричных шифров, что позволит более взвешенно подходит к их проектированию.

Литература

1. Vaudenay, S. Decorrelation: a theory for block cipher security [Text] / S. Vaudenay // Journal of Cryptology. – 2003. – Vol. 16, Issue 4. – P. 249–286. doi: 10.1007/s00145-003-0220-6
2. Luby, M. How to construct pseudorandom permutations from pseudorandom functions [Text] / M. Luby, C. Rackoff // SIAM Journal on Computing. – 1988. – Vol. 17, Issue 2. – P. 373–386. doi: 10.1137/0217022
3. Maurer, U. M. A simplified and generalized treatment of Luby-Rackoff pseudorandom permutation generators [Text] / U. M. Maurer // Advances in Cryptology – EUROCRYPT'92 : proceedings of the Workshop on the Theory and Application of of Cryptographic Techniques, Balatonf red, Hungary. – Berlin ; Heidelberg : Springer, 1993. – P. 239–255.
4. Олейников, Р. В. Уточнение эффективности различения цепи Фейстеля и случайной перестановки [Текст] / Р. В. Олейников, Д. С. Кайдалов // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2011. – Вып. 167. – С. 190–202.
5. Олейников, Р. В. Оценка сложности различения схемы Лей-Месси и случайной перестановки [Текст] / Р. В. Олейников, Д. С. Кайдалов // Прикладная радиоэлектроника. – 2012. – Т. 11, № 2. – С. 152–159.
6. Patarin, J. Security of random Feistel schemes with 5 or more rounds [Text] / J. Patarin // Advances in Cryptology – CRYPTO 2004 : proceedings of the 24th Annual International CryptologyConference, Santa Barbara, California, USA. – Berlin ; Heidelberg : Springer, 2004. – P. 106–122.
7. Patarin, J. Generic attacks on Feistel schemes [Text] / J. Patarin // Advances in Cryptology – ASIACRYPT 2001 : proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia. – Berlin ; Heidelberg : Springer, 2001. – P. 222–238.
8. Patarin, J. About Feistel schemes with six (or more) rounds [Text] / J. Patarin. – Lecture Notes in Computer Science, 1998. – P. 103–121. doi: 10.1007/3-540-69710-1_8
9. Vaudenay, S. On the Lai-Massey Scheme [Text] / S. Vaudenay. – Lecture Notes in Computer Science, 1999. – P. 8–19. doi: 10.1007/978-3-540-48000-6_2
10. Шеннон, К. Теория связи в секретных системах [Текст] / К. Шеннон. – Работы по теории информации и кибернетике. М., 1963. – С. 333–369.
11. Gilbert, H. Super-Sbox Cryptanalysis: Improved Attacks for AES-like permutations [Electronic resource] : report 2009/531 / H. Gilbert, T. Peyrin. – Cryptology ePrint Archive, 2009. – Available at: https://eprint.iacr.org/2009/531.pdf