УДК 004:003.26

НЕКОТОРЫЕ ПОДХОДЫ К ДИФФЕРЕНЦИАЛЬНОМУ АНАЛИЗУ УПРОЩЕННОГО ШИФРА MISTY1

Ищукова Е.А., Куликов А.В.

Южный федеральный университет, Таганрог, e-mail: uaishukova@sfedu.ru

В статье рассмотрены подходы к построению разностных характеристик для оценки надежности шифра MISTY1 с использованием дифференциального метода криптоанализа. Шифр MISTY1 был разработан в 1995 г. и представлен проектом NESSIE в качестве рекомендованного криптографического примитива в 2003 г. Данный алгоритм шифрования основан на вложенных схемах Фейстеля. В результате работы были проанализированы таблицы замены, а также три уровня вложенности функций шифра MISTY1(FO, FI и основная функция). Для уменьшенного до четырех раундов шифра, без FL функций были составлены разности, с помощью которых возможно получить правильные пары текстов и с помощью формул получить все подключи. В то время как перебор грубой силой будет выполнять 2^{128} вариантов ключа, с помощью дифференциального анализа достаточно перебора не более 2^{44}. В результате работы были проанализированы основные элементы шифра MISTY1. Предложена схема построения разностных характеристик для четырехраундового упрощенного шифра MYSTI1. Разработаны алгоритмы и реализованы программы по поиску правильных пар текстов и вычисления битов секретного ключа на основе использования разработанных схем.

Ключевые слова: криптография, блочный шифр, MISTY1, дифференциальный анализ, разность текстов

SOME APPROACHES TO THE DIFFERENTIAL ANALYSIS OF THE SIMPLEFIED VERSION OF MISTY1 CIPHER

Ishchukova E.A., Kulikov A.V.

Southern Federal University, Taganrog, e-mail: uaishukova@sfedu.ru

The article discusses approaches to constructing difference characteristics for estimating the reliability of the MISTY1 cipher using the differential cryptanalysis method. The MISTY1 cipher was developed in 1995 and is presented by the NESSIE project as the recommended cryptographic primitive in 2003. This encryption algorithm is based on Feistel schemes. As a result of the work, the replacement tables were analyzed, as well as three levels of nesting of the MISTY1 cipher functions (FO, FI and the main function). For a reduced to four rounds of cipher, without FL functions, differences were compiled, with which it is possible to get the correct pairs of texts and using formulas to get all the subkeys. While the brute-force search will perform 2^{128} variants of the key, with the help of differential analysis, it is enough to search no more than 2^{44}. As a result of the work, the main elements of MISTY1 cipher were analyzed. A scheme for constructing the difference characteristics for the four-round simplified cipher MYSTI1 is proposed. Programs have been developed and implemented to find the correct pairs of texts and calculate the bits of the secret key based on the use of the developed schemes.

Keywords: cryptography, block cipher, MISTY1, differential analysis, text difference

Шифр MITSY1 был представлен на конкурс проектов NESSIE и стал одним из трех победителей в категории симметричных блочных шифров [1]. Подробное описание шифра можно найти в обзоре С. Панасенко [2]. Шифр MITSY1 интересен еще и тем, что позже он был представлен на конкурс CRYPTREC по выбору криптостандарта Японии и вошел в состав шифров-победителей [3]. В настоящей работе рассматривается возможность применения метода дифференциального анализа к упрощенной версии шифра MISTY1. При проведении исследований стойкости современных шифров часто применяется практика рассмотрения упрощенных версий шифров. Это делается для детального и более подробного изучения отдельных компонентов шифра с тем, чтобы в дальнейшем иметь возможность перейти к рассмотрению полной версии шифра.

Алгоритм MISTY1 основан на «вложенных» сетях Фейстеля. Сначала 64-битный шифруемый блок данных разбивается на два 32-битных подблока, после чего выполняется r раундов следующих преобразований (рис. 1). В нечетных раундах каждый подблок обрабатывается функцией FO. Правый подблок складывается по модулю два с левым подблоком, прошедшим через функцию FO. Подблоки меняются местами. После заключительного раунда оба подблока обрабатываются операцией FL.

Операция FL работает следующим образом (рис. 1). Обрабатываемый 32-битный блок разбивается на два 16-битных подблока. Сначала правая часть блока складывается по модулю два с результатом операции «логическое И» для левой части блока и одним из подключей. После этого левая часть исходного блока складывается по модулю два с результатом операции «Логическое ИЛИ» для преобразованной правой части и второго подключа.

Операция FO представляет собой функцию вложения второго уровня (рис. 1). Здесь

выполняется разбиение входного блока на два равных фрагмента по 16 бит, которые проходят 3 раунда следующих преобразований. Левая половина блока складывается по модулю два (операцией XOR) с раундовым подключом $KO_{i,k}$, где k – номер раунда функции FO. После этого левая часть блока преобразуется с помощью операции FI. Левая половина блока складывается по модулю два (XOR) с правой половиной блока. После этого левая и правая половины меняются местами. После последнего раунда левая часть блока складывается по модулю два (XOR) с последним подключом $KO_{i,k}$.

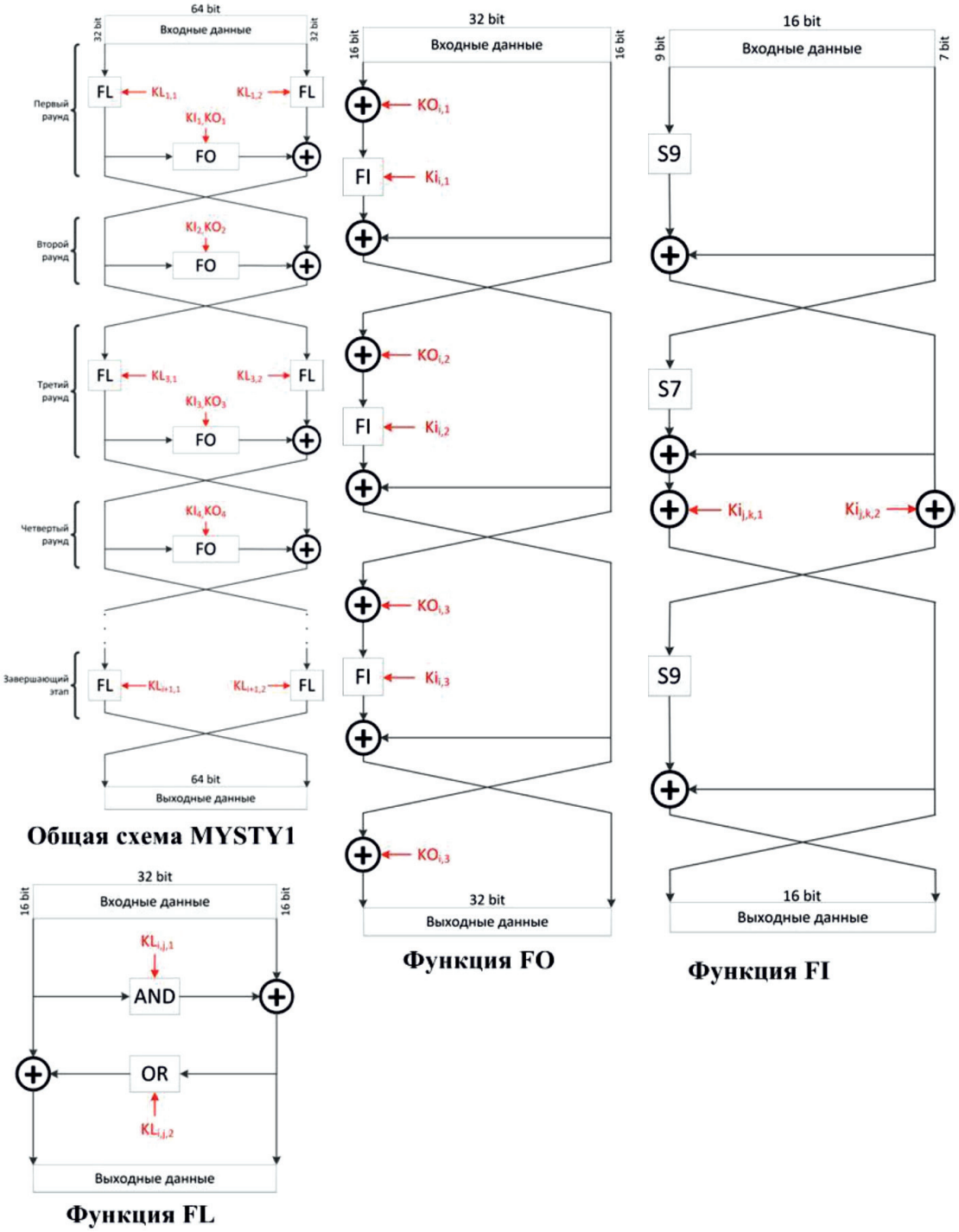


Рис. 1. Структура шифра MYSTY1

Операция FI представляет собой третий уровень вложенности сети Фейстеля (рис. 1). В данном случае сеть Фейстеля является несбалансированной, так как левая и правая части сети имеют разное количество обрабатываемых битов. Обрабатываемый блок делится на два подблока длиной 9 и 7 бит (левая и правая части). Затем выполняются 3 раунда следующих преобразований. Левая часть проходит через S-блок замены. При этом в 1 и 3 раундах левая часть содержит 9 битов и обрабатывается таблицей S9, во втором раунде левая часть содержит 7 битов и обрабатывается таблицей S7. После этого левая часть блока складывается с правой частью по модулю два (операция XOR). При этом, если справа расположена 7-битная часть, то она дополняется нулями слева до 9 бит. Если же справа расположена 9-битная часть, то у нее не учитываются два старших бита (слева). Во втором раунде левая часть блока складывается по модулю два (операция XOR) с раундовым подключом $KI_{i,k,1}$, а правая часть блока – с подключом $KI_{i,k,2}$. В остальных раундах эти действия не выполняются. После этого левая и правая части меняются местами.

Расшифрование производится выполнением тех же операций, но со следующими изменениями. Фрагменты расширенного ключа используются в обратной последовательности. Вместо функции FL используется обратная ей функция FL^{-1}.

Подключи вырабатываются согласно схеме, изображенной на рис. 2. Ключ длиной 128 бит делится на 8 подключей по 16 бит и каждая из них подается на вход блока FI, а в качестве ключа подается следующий подключ. Для последнего подключа, подаваемого как текст, в качестве ключа подается первый подключ. Красными линиями обозначена подача ключа в блок FI. Получившиеся подключи обозначаются штрихом. Необходимые фрагменты расширенного ключа «набираются» согласно таблице и используются во всех функциях шифра MYSTY1 (рис. 1).

Метод дифференциального криптоанализа впервые был предложен в начале 1990-х гг. Э. Бихамом и А. Шамиром для анализа алгоритма шифрования DES. Хотя в книге Б. Шнайера упоминается о том, что разработчики алгоритма DES знали о возможности такого анализа еще во время разработки алгоритма в 1970-х гг., широкая общественность узнала о дифференциальном криптоанализе именно из работ [4, 5]. С помощью метода дифференциального криптоанализа сложность анализа алгоритма DES сократилась до 2^{37}. Дальнейшее развитие этого метода показало возможность его применения к целому классу различных видов шифров, позволило выявить слабые места многих используемых и разрабатываемых алгоритмов шифрования. Сегодня этот метод, а также некоторые его производные, такие как метод линейно-дифференциальный, метод невозможных дифференциалов, метод бумеранга, широко используются для оценки стойкости вновь создаваемых шифров [6].

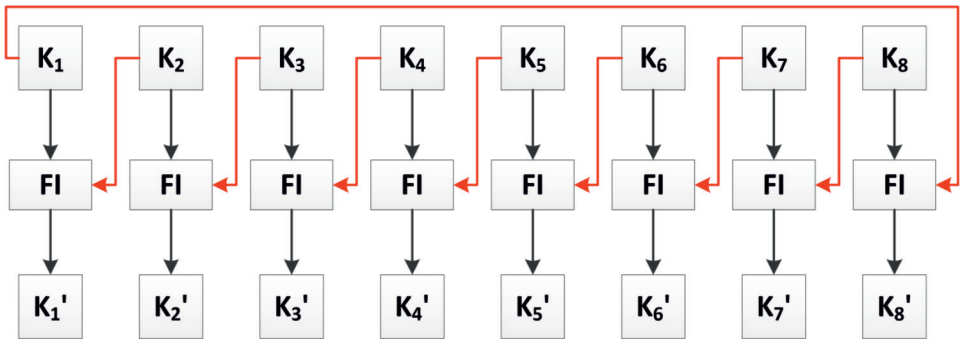


Рис. 2. Схема выработки подключей

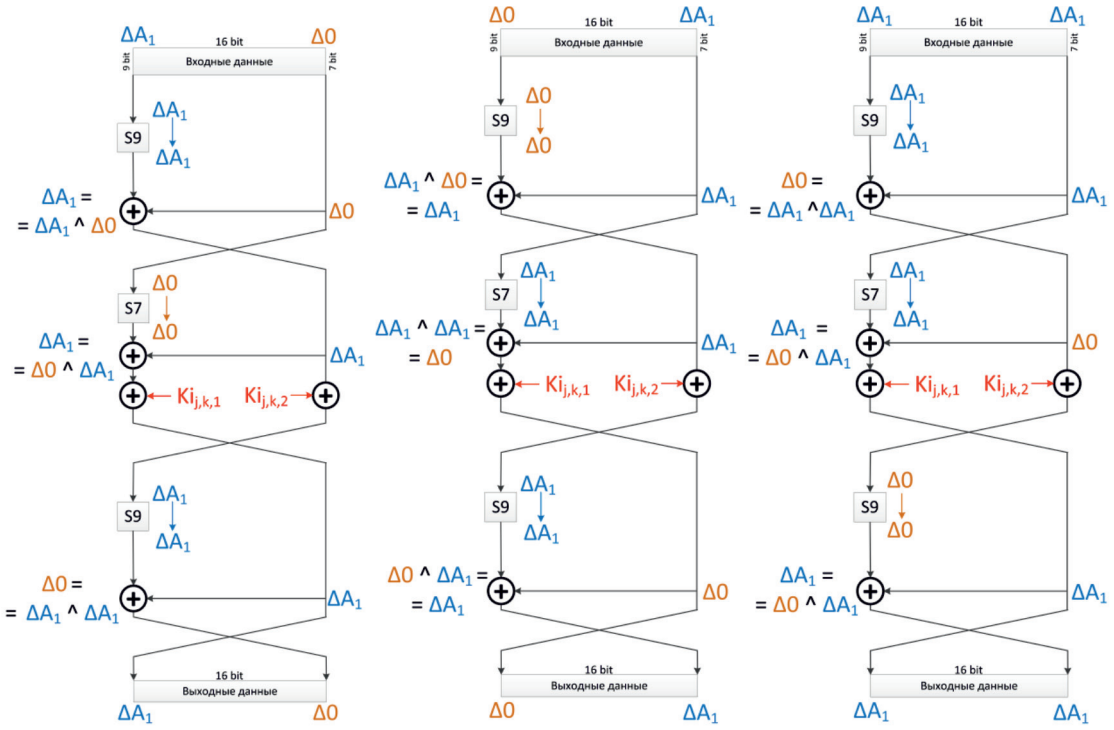
Выборка подключей

Назначение	$KO_{i,1}$	$KO_{i,2}$	$KO_{i,3}$	$KO_{i,4}$	$KI_{i,1}$	$KI_{i,2}$	$KI_{i,3}$
Фрагмент	K_i	K_{i+2}	K_{i+7}	K_{i+4}	K'_{i+5}	K'_{i+1}	K'_{i+3}
Назначение	$KL_{i,1,1}$	$KL_{i,2,1}$	$KL_{i,1,2}$	$KL_{i,2,2}$			
Фрагмент	$K_{(i+1)/2}$	$K'_{(i+1)2+2}$	$K'_{(i+1)2+6}$	$K_{(i+1)2+4}$			

Анализ S-блоков. Число раундов MISTY1 должно быть всегда кратным 4, рекомендуемым же является MISTY1 с 8 раундами. В целях наилучшего понимания механизмов шифра и его подверженности дифференциальным атакам на старте были приняты следующие решения. Рассматривать упрощенную модель MISTY1. Для этого убрать из алгоритма шифра все FL-функции. Сократить рекомендуемые 8 раундов до четырех (тем самым мы не будем нарушать целостности шифра, которая также обеспечивается кратностью, но проанализируем более короткую версию шифра).

Начальными элементами, от которых следует отталкиваться при дифференциальном анализе, являются нелинейные блоки. В шифре MYSTY1 есть два блока замены: S7 и S9. Первый этап дифференциального анализа заключался в построении таблиц вероятностей для этих блоков замен. Таблица вероятности представляет собой по горизонтали входящую разность текстов, по вертикали – выходящую разность текстов, а на пересечении вероятность соответствия выходной разности заданной входной разности. Алгоритм анализа дифференциальных свойств нелинейных блоков приведен в работе [7]. В результате анализа было показано, что любая входная разность текстов приводит к любой выходной разности либо с вероятностью 0, либо с вероятностью 2 к 128 или 512 соответственно для блоков S7 и S9. Также важно отметить, что входная разность, равная нулю, с вероятностью 100% даст на выходе S-блока также нулевую разность.

Анализ функции FI. При анализе функции FI было сделано предположение, что есть такая разность ΔA, которая может отразиться сама в себя. То есть $S9(\Delta A) = S7(\Delta A) = \Delta A$. Для подтверждения этого факта был разработан алгоритм и проанализированы таблицы с вероятностями для входных-выходных разностей блоков S7 и S9. После анализа S-блоков было обнаружено 33 варианта ΔA, которая отражалась бы сама в себя. На рис. 3 показаны три варианта прохождения входной разности через функцию FI, в случае, когда значение разности после S-преобразования остается неизменным. В первом варианте (рис. 3, а) левая половина разности равна значению ΔA_1, правая часть разности равна нулю ($\Delta 0$). Во втором варианте (рис. 3, б) левая половина разности равна нулю ($\Delta 0$), а правая часть разности равна значению ΔA_1. В третьем варианте (рис. 3, в) обе части разности равны значению ΔA_1. Для дальнейшего анализа мы будем использовать второй вариант схемы, приведенный на рис. 3, б.



а) *б)* *в)*

Рис. 3. Различные схемы преобразования разностей с помощью функции FI

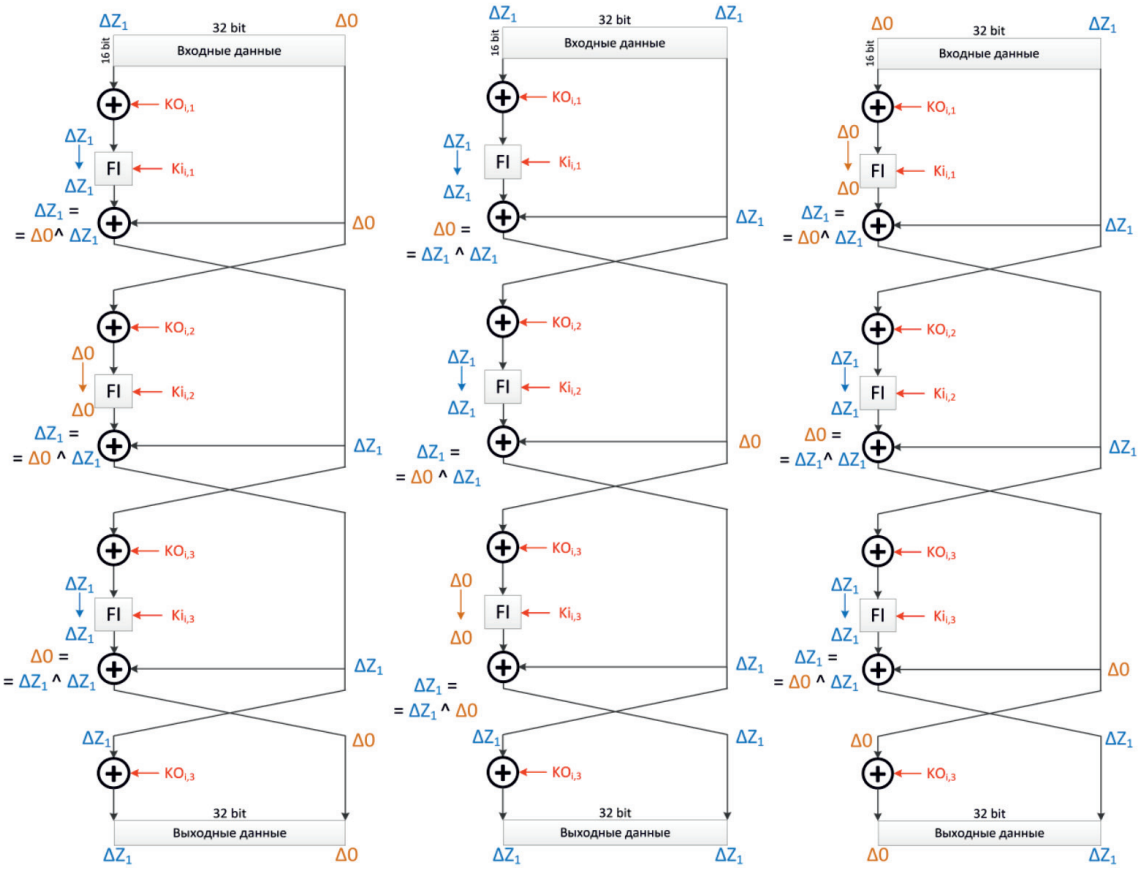


Рис. 4. Различные схемы преобразования разностей с помощью функции FO

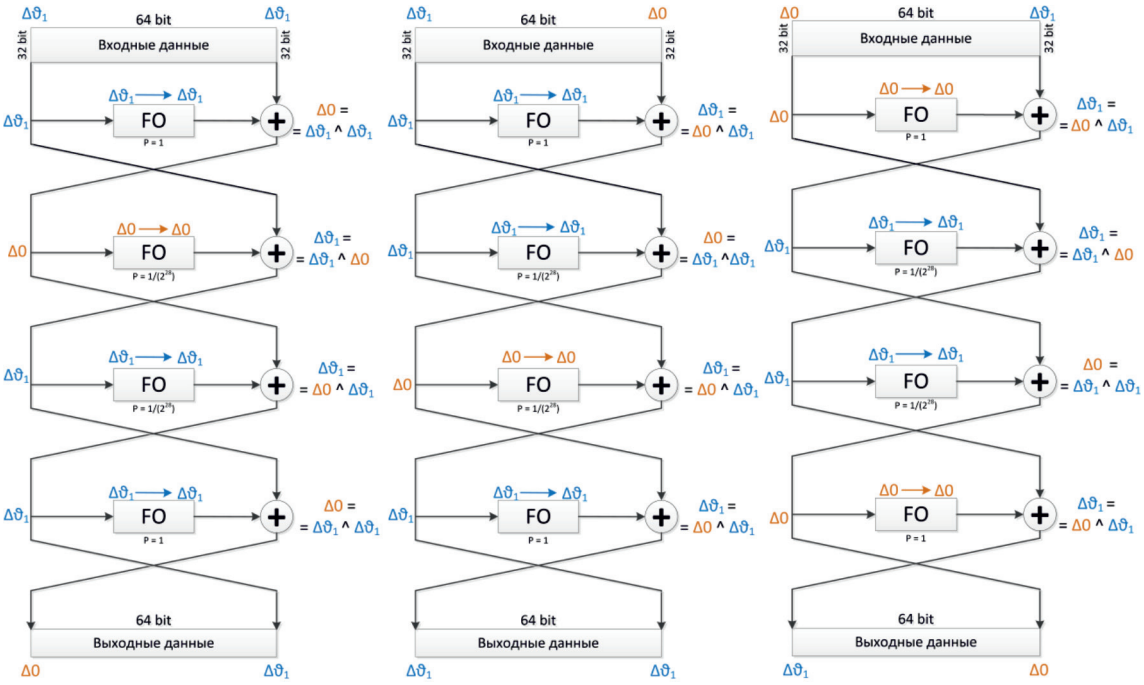


Рис. 5. Различные схемы преобразования разностей для 4 раундов шифра MISTY1

Анализ функции FO. Для построения разностных схем функции FO можно использовать тот же принцип, что и для функции FI. Будем рассматривать случаи, когда преобразование FI оставляет входную разность неизменной. Нами было рассмотрено несколько вариантов построения подобных схем, три из которых представлены на рис. 4. При выборе схемы для дальнейшего анализа мы руководствовались тем, какую ключевую информацию нам позволит извлечь рассматриваемая схема. Так, схема, приведенная на рис. 4, в, позволит нам определить только ключ $KO_{i,2}$. Вариант, представленный на рис. 4, а, даст нам возможность найти ключи $KO_{i,1}$ и $KO_{i,3}$, но строго последовательно, т.е. мы сможем найти $KO_{i,3}$ и $KI_{i,3}$ только после того, как найдем $KO_{i,1}$ и $KI_{i,1}$. Вариант, представленный на рис. 4, б позволяет найти ключи $KI_{i,2}$, $KO_{i,2}$ и $KI_{i,1}$, $KO_{i,1}$ независимо друго от друга. Поэтому дальнейший анализ основывается на схеме, представленной, на рис. 4, а.

Анализ основной функции MISTY1. Для построения схем отображения разностей при выполнении основного преобразования шифра MISTY1, был использован эффект отражения разности в самой себя. При построении разностей учитывались те варианты, которые позволяют получить максимальную вероятность дифференциала (то есть определение выходной разности, вероятность получения которой является максимально возможной). Наиболее подходящие схемы из всех рассмотренных схем при выполнении анализа представлены на рис. 5.

Исходя из вариантов, представленных на рис. 5, можно определить, какую часть секретного ключа можно будет определить с использованием данных разностных схем. Так, с помощью схемы, представленной на рис. 5, а, можно проанализировать блоки FO_1 и FO_4 параллельно. Блок FO_2 не может быть подвергнут анализу из-за нулевой разности, а блок FO_3 из-за того, что он зависит от блока FO_2. С помощью схемы, представленной на рис. 4, б, можно независимо проанализировать блоки FO_1, FO_4. После этого можно будет извлечь информацию из блока FO_2. Блок FO_3 придется пропустить из-за нулевой разности. Схема, представленная на рис. 5 в, является самой малоинформативной, так как имеет в своем составе сразу два блока с нулевой разностью. Выбирая между схемами, представленными на рис. 4, а и б, стоит учесть, что для схемы 4, а, подбор подключей будет проводиться по первому и последнему раунду, а для схемы 4, б, – по первому и второму (последовательно). При этом вероятность нахождения правильных пар текстов для обеих схем составит $\frac{1}{2^{28}} * \frac{1}{2^{28}} * \frac{1}{2^{28}} = \frac{1}{2^{84}}$.

В связи с тем, что для поиска правильных пар текстов, удовлетворяющих заданным вероятностям, необходимо проанализировать большое количество пар текстов, в данном случае целесообразно использовать технологии распределенных многопроцессорных вычислений, такие как MPI и NVIDIA CUDA [8, 9]. Согласно Парадоксу Дней Рождений [10], проанализировав 2^{42} пар текстов, можно найти правильную пару текстов с вероятностью $p = 0{,}5$. Экспериментальные данные при поиске дифференциалов для шифра MYSTI1 на основе технологии MPI были получены с использованием семи двухъядерных вычислительных узлов Intel Core i5 – 3320M CPU, 2.60 GHz, 4 Gb RAM. Среднее время обработки 2^{42} пар текстов с использованием 14 процессоров составило в среднем 900 часов (15 дней). При использовании технологии NVIDIA CUDA вычисления производились на ПК Intel i5 2400 NVIDIA GTS 459 8 Gb RAM. Было показано, что при количестве процессоров, равном 1024, среднее время вычислений составляет 640 минут (около 11 часов).

В заключительном этапе анализа был реализован алгоритм поиска битов секретного ключа. Так, для схемы 5, б, был предложен алгоритм, состоящий из трех этапов. На первом этапе, анализируя значения разностей, аналитик может восстановить раундовые подключи K_1, K_3, K_4, K_8 и K'_1, K'_4, K'_6, K'_7. На втором этапе, используя уже найденные значения подключей, аналитик может восстановить связанные с ними раундовые подключи: K_2, K_5, K_7 и K'_3, K'_8. К сожалению, в данном случае нельзя получить информацию о раундовых подключах K_6 и K'_2, K'_5 – их можно определить только перебором.

Работа выполнена при поддержке гранта РФФИ № 17-07-00654-а.

Список литературы

1. Алгоритмы шифрования – участники конкурса NESSIE. Часть 1 [Электронный ресурс]. – Режим доступа: http://www.ixbt.com/soft/nessie-part1.shtml (дата обращения: 01.02.18).

2. Панасенко С. NESSIE – конкурс криптоалгоритмов [Электронный ресурс]. – Режим доступа: http://www.panasenko.ru/Articles/63/63.html (дата обращения: 01.02.18).

3. Панасенко С. CRYPTREC – проект по выбору криптостандартов Японии [Электронный ресурс]. – Режим доступа: http://www.panasenko.ru/Articles/156/156.html (дата обращения: 01.02.18).

4. Biham E., Shamir A. Differential Cryptanalysis of the Full 16-round DES. – Advances in Cryptology. – Crypto'92, Springer-Velgar, 1998. – P. 487–496.

5. Biham E., Shamir A.: Differential Cryptanalysis of DES-like Cryptosystems, Extended Abstract. – Crypto'90. – Springer-Velgar, 1998. – 105 p.

6. Ищукова Е.А. Дифференциальный анализ шифра Кузнечик / Е.А. Ищукова, Л.К. Бабенко, Е.А. Толоманенко // Известия ЮФУ. Технические науки. – Таганрог: Изд-во ЮФУ, 2017. – № 5. – С. 25–37.

7. Ищукова Е.А. Дифференциальные свойства S-блоков замены для алгоритма ГОСТ 28147-89 / Е.А. Ищукова, И.А. Калмыков // Инженерный вестник Дона. – 2015. – № 4 [Электронный ресурс]. – Режим доступа: ivdon.ru/ru/magazine/archive/n4y2015/3284 (дата обращения: 01.02.18).

8. Бабенко Л.К. Применение параллельных вычислений при решении задач защиты информации / Л.К. Бабенко, Е.А. Ищукова, И.Д. Сидоров // Программные системы: теория и приложения. – 2013. – Т. 4, № 3–1 (17). – С. 25–42.

9. Сандерс Дж. Технология Cuda. Введение в программирование графических процессоров / Дж. Сандерс, Э. Кэндрот. – М.: ДМК Пресс, 2015. – 232 с.

10. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходный код на С / Б. Шнайер. – М.: Изд-во Вильямс, 2017. – 1040 с.