УДК 004.021

НЕКОТОРЫЕ ПОДХОДЫ К АНАЛИЗУ ШИФРА МАГМА+ С ИСПОЛЬЗОВАНИЕМ МЕТОДА НЕВОЗМОЖНЫХ ДИФФЕРЕНЦИАЛОВ

Ищукова Е.А., Письменский М.В., Бабенко Л.К.

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

Данная статья посвящена разработке и исследованию алгоритмов для проведения анализа алгоритма Магма с использованием метода невозможных дифференциалов. В работе рассмотрены дифференциальные свойства S-блоков замены, рекомендованных к использованию в шифре Магма в рамках стандарта ГОСТ Р34.12-2015. Анализ блоков позволил выявить дифференциальные свойства, с помощью которых стало возможным построение 8-раундовой разностной характеристики с использованием метода невозможных дифференциалов. Применение полученной характеристики позволило получить биты секретного ключа, используемые в первом раунде шифрования, для ненулевых блоков разности. На основе предложенного подхода был разработан, реализован и экспериментально проверен алгоритм поиска ключа. Используя предложенную технику, можно проводить анализ для поиска различных фрагментов секретного ключа, используя для каждой итерации схему со смещением ненулевых блоков в исходной разности на n блоков. Показано, что переход от шифра Магма+ к шифру Магма приведет к понижению вероятности анализа. Дальнейшим направлением исследований является переход к рассмотрению большего количества раундов в рамках рассматриваемого метода анализа.

Ключевые слова: криптография, блочный шифр, Магма, ГОСТ Р34.12-2015, фиксированные блоки замены, невозможные дифференциалы

SOME APPROACHES TO THE ANALYSIS OF THE CIPHER MAGMA + WITH THE METHOD OF AN IMPOSSIBLE DIFFERENTIALS

Ischukova E.A., Pismensky M.V., Babenko L.K.

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

This article is dedicated to the development and study of an algorithms for the analysis of cipher Magma+ with the method of an impossible differentials. The paper discusses the differential properties of the S-boxes, recommended for the cipher Magma within GOST R34.12-2015. Differential properties were revealed by analysis of S-boxes. So it became possible to build the 8-round characteristics of the difference using the method of an impossible differentials. Some bits of the secret key used in the first round were obtained by application of this characteristics. This bits were used in the non-zero blocks of the difference. Key search algorithm was developed, implemented and experimentally verified on the basis of this approach. It is possible to analyze the various fragments of the secret key by using for each iteration nonzero offset circuit blocks in the original difference by n blocks. It is shown that the transition from cipher Magma+ to cipher Magma will lead to a decrease of the analysis probability. A further area of our research is the transition to the consideration of a larger number of rounds within the method of impossible differentials.

Keywords: cryptography, a block cipher, Magma, GOST R34.12-2015, fixed S-boxes, impossible differentials

Алгоритм шифрования Магма представляет собой блочный алгоритм шифрования, построенный по схеме Фейстеля. Ранее этот шифр был известен как ГОСТ 28147-89. Однако с 1 января 2016 года он вошел в состав нового стандарта симметричного блочного шифрования ГОСТ Р.34.12 – 2015 под названием Магма [4]. Единственное отличие шифра Магма от шифра ГОСТ 28147-89 заключается в том, что теперь у этого шифра зафиксированы блоки замены. Магма преобразует 64-битовые блоки данных и использует при шифровании 256-битовый ключ, что сразу значительно повышает стойкость данного алгоритма к методу полного перебора. Ранее для алгоритма ГОСТ 28147-89 блоки замены не являлись фиксированным элементом и могли быть выбраны произвольным образом. Считается, что даже при выборе слабых блоков 32 раундов алгоритма шифрования ГОСТ будет достаточно для того, чтобы обеспечить требуемую стойкость. Известны блоки замены, которые использовались в приложении для Центрального Банка РФ, однако до сих пор нет каких-либо сведений об анализе алгоритма даже с имеющимися известными данными. Отдельно стоит отметить, что буквально два месяца назад в нашей стране был утвержден новый стандарт шифрования данных ГОСТ 34.12-2015, который вступает в силу с 1 января 2016 года. Данный стандарт содержит два алгоритма шифрования, одним из которых является алгоритм шифрования ГОСТ28147-89, для которого зафиксированы блоки замены. Ранее в диссертационной работе Е.А. Ищуковой рассматривались дифференциальные свойства для алгоритма шифрования ГОСТ 28147-89 как с известными блоками замены, так и с блоками замены, выбранными произвольным образом [3]. В настоящей работе мы в первую очередь рассмотрим блоки замены, выбранные для нового стандарта ГОСТ Р34.12-2015. После этого уделим

особое внимание разработке универсального алгоритма поиска невозможных дифференциалов. В данной работе будет рассмотрен алгоритм Магма, в котором операция сложения по модулю 2^{32} заменена на побитовое сложение по модулю 2. Однако при этом будут рассмотрены дифференциальные свойства операции сложения по модулю 2^{32} и рассмотрен способ перехода от операции сложения по модулю 2 к операции сложения по модулю 2^{32}.

Алгоритм шифрования Магма является симметричным блочным шифром, построенным по типу сети Фейстеля, с размером секретного ключа 256 бит, размером входного сообщения 64 бита и 32 раундами шифрования. При шифровании алгоритмом Магма 64-битный блок исходного текста разбивается на две половины – левую и правую часть. Ключ шифрования разбивается на 8 подключей, по 32 бита каждый. В ходе процесса шифрования ключи с 1 по 24 раунд циклически повторяются K1 – K8, а затем с 25-го по 32-й раунд ключи инвертируются и имеют вид K8 – K1. После выполнения 32 раундов шифрования левая и правая части «склеиваются», образуя результат работы алгоритма – блок шифр-текста. Расшифрование выполняется аналогично, изменяется лишь порядок ключей – он инвертируется относительно зашифрования.

На рис. 1 представлены общая схема алгоритма шифрования и содержимое функции F.

Как отмечалось выше, шифр Магма имеет фиксированный вид блоков замены, приведенный в табл. 1.

Метод невозможных дифференциалов – метод криптоанализа блочных шифров, предложенный Эли Бихамом, Эди Шамиром и Алексом Бирюковым в 1998 году. Его применяли ко многим усеченным версиям шифров [5–7]. Суть метода заключается в нахождении двух таких последовательностей для прохождения разностей через этапы шифра, чтобы вероятность их возникновения вместе была равна нулю(невозможна). Если такие последовательности могут быть найдены, то, добавив первый раунд, можно выполнить перебор ключей. Все ключи, которые приводят к невозможным ситуациям, являются неверными. Этот метод позволяет отбросить неверные ключи или биты ключа.

Анализ любого алгоритма шифрования начинается с анализа его составных частей, то есть с анализа тех криптографических примитивов, которые могут оказать хоть какое-нибудь влияние на изменение разности в процессе ее прохождения через раунды алгоритма. Поэтому для начала необходимо исследовать свойства основных компонентов алгоритма Магма: циклического сдвига влево на 11 позиций, сложения по модулю 2, сложения по модулю 2^{32} и замены данных с помощью S-блоков замены. В работе [3] были рассмотрены дифференциальные свойства для вышеуказанных операций. Не будем останавливаться подробно на детальном анализе, а просто сформулируем выявленные закономерности. Известно, что операция сложения по модулю два не влияет на значение разности, поэтому при построении разностных характеристик данная операция не учитывается. Для операции циклического сдвига работает следующее правило:

$$(A \ll 11) \oplus (B \ll 11) = (A \oplus B) \ll 11),$$

то есть для получения правильной разности на выходе операции циклического сдвига необходимо входную разность циклически сдвинуть влево на 11 позиций. Для операции сложения по модулю 2^n: $(a + b) \bmod 2^n$ были выявлены следующие правила:

1. Любое значение входной разности может отобразиться само в себя, то есть остаться неизменным. Вероятность такого отображения определяется следующим образом: если входная разность $\Delta вх < 2^{n-1}$, то $p = \frac{1}{2^k}$; если входная разность $\Delta вх \geq 2^{n-1}$, то $p = \frac{1}{2^{k-1}}$, где k – число ненулевых позиций входной разности.

Таблица 1

Блоки замены для функции F шифра Магма

S8	12	4	6	2	10	5	11	9	14	8	13	7	0	3	15	1
S7	6	8	2	3	9	10	5	12	1	14	4	7	11	13	0	15
S6	11	3	5	8	2	15	10	13	14	1	7	4	12	9	6	0
S5	12	8	2	1	13	4	15	6	7	0	10	5	3	14	9	11
S4	7	15	5	10	8	1	6	13	0	9	3	14	11	4	2	12
S3	5	13	15	6	9	2	12	10	11	7	8	1	4	3	14	0
S2	8	14	2	5	6	9	1	12	15	4	11	0	13	10	3	7
S1	1	7	14	13	0	5	8	3	4	15	10	6	9	12	11	2

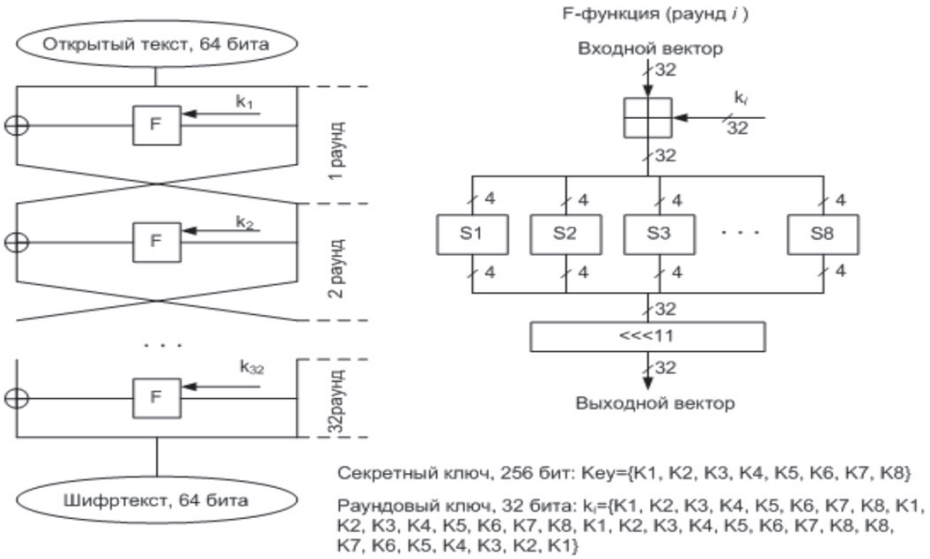

Рис. 1. Общая схема шифрования и содержимое функции F

2. Для входной разности = 0 на выходе преобразования будет значение выходной разности $\Delta вx = 0$ с вероятностью $p = 1$.

3. Для входной разности $\Delta вx = 2^{n-1}$ на выходе преобразования будет значение выходной разности $\Delta вx = 2^{n-1}$ с вероятностью $p = 1$.

Отдельно остановимся на рассмотрении дифференциальных свойств S-блоков замен. Согласно стандарту [4] для алгоритма ГОСТ утвержден набор блоков замены, приведенный в табл. 1. В соответствии с [4] в данной интерпретации (в стандарте данные блоки обозначены как π и имеют нумерацию от 0) блок S1 применяется к самому младшему байту, а S8 – к самому старшему байту рассматриваемого блока данных.

Алгоритм построения таблиц анализа для выявления дифференциальных свойств S-блоков замены был разработан ранее и описан в работе [1]. С использованием этого алгоритма, были построены и проанализированы таблицы анализа для каждого S-блока замены. Результаты анализа представлены в работе [2].

Для анализа шифра Магма с помощью метода невозможных дифференциалов необходимо провести анализ раундовых преобразований алгоритма и посмотреть, как изменяются разности текстов после прохождения этих преобразований. Для данного шифра будем учитывать разности в полубайтах, приходящих на вход блоках замены, а не в отдельных битах.

При построении графических схем для разностных характеристик будем использовать следующие обозначения: черным цветом будем обозначать полубайты, в которых есть разности, полубайты белым цветом – полубайты с нулевой разностью, красным цветом полубайты с неизвестной разностью, синим цветом – полубайт, в котором разность равна 9.

Для побитового сдвига на 11 позиций влево разность текстов сдвигается на 11 позиций. Если рассматривать разности в полубайтах, а не в отдельных битах, то это означает, что после операции сдвига количество блоков замены, в которых присутствует разность, может увеличиться. Например, разность в третьем блоке может дать разности и в пятом и в шестом блоке, как показано на рис. 2.

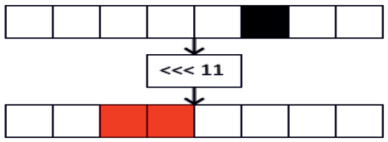

Рис. 2. Пример изменения разности для циклического сдвига

Зная, как проходят разности двух текстов через преобразования алгоритма, а также опираясь на дифференциальные свойства алгоритма шифрования Магма, можно построить дифференциальную последовательность для шести раундов алгоритма Магма так, как показано на рис. 3.

Это возможно за счет использования дифференциальной особенности, найденной для шестого S-блока, которая заключается в том, что входная разность $\Delta A = 9$ при-

ведет к разностям ΔC, у которых младший бит всегда будет равен 0. Это значит, что даже после сдвига на 11 позиций, разность затронет всего один полубайт [2].

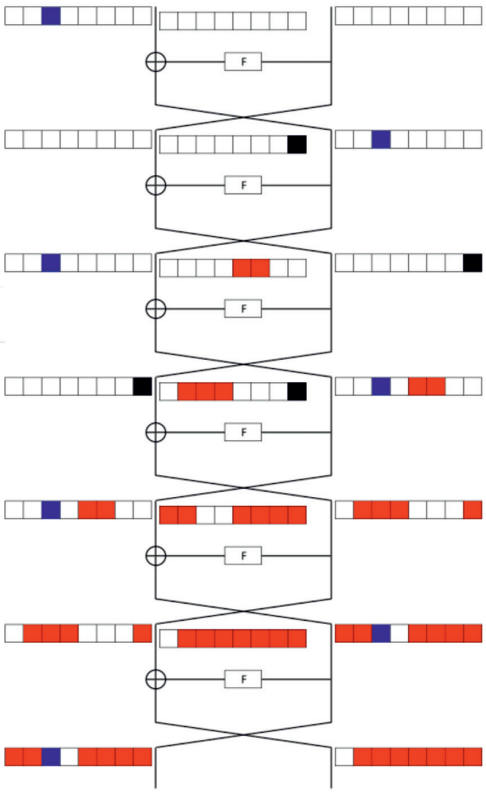

Рис. 3. Схема для шести раундов

Для проведения анализа необходимо построить ещё одну дифференциальную последовательность, которая будет выполняться с вероятностью 0, если выполняется первая последовательность. Чтобы найти вторую последовательность, нужно рассмотреть, как проходят разности через преобразования при расшифровании. Такая последовательность, состоящая из одного раунда шифрования, представлена на рис. 4.

Имея две эти последовательности, можно их объединить для построения разностной характеристики невозможных дифференциалов. Полная схема с добавленным первым раундом показана на рис. 5. Используя эту схему, можно приступить к поиску подключей. Для этого необходимо добавить первый раунд, который может привести к первой последовательности при некоторых ключах. Для шифрования данных будем использовать упрощенный алгоритм Магма, усеченный до 8 раундов шифрования, в котором операция сложения с раундовым подключом осуществляется по модулю 2. Для нахождения ключей необходимо проанализировать зашифрованные пары текстов, имеющие разность в первом полубайте левой половины, и разность, равную девяти, в шестом полубайте в правой половине. В результате анализа будут отобраны только те пары текстов, которые точно не имеют разности в шестом полубайте левой половины и третьем и четвертом полубайте правой половины. После этого необходимо проверить все возможные биты ключа в первом полубайте и отбросить те ключи, которые приводят к разностям только в шестом полубайте в левой половине после первого раунда. Таким образом, можно определить возможные значения той части секретного подключа, которая приходится на сложение с первым полубайтом, то есть 4 бита от исходного секретного ключа. На основе предложенного подхода был разработан алгоритм поиска возможных значений секретного ключа для упрощенного 8-раундового алгоритма Магма.

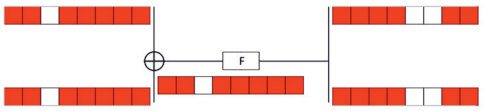

Рис. 4. Схема для одного раунда

Разработанный алгоритм был реализован на языке программирования C. Для проведения эксперимента использовался компьютер с процессором Intel Core i5-4210M 2.60 GHz и с 8 ГБ оперативной памяти.

Таблица 2

Результаты экспериментов

Ключ	Всего текстов	Количество подходящих тестов	Количество неправильных ключей	Время, секунды
9437184	5244925	1000	6	5,22
3145728	3000669	1000	8	4,37
60817408	3001081	1000	2	4,43
60817439	4198785	1000	10	4,54
102773567	2332176	1000	8	3,76

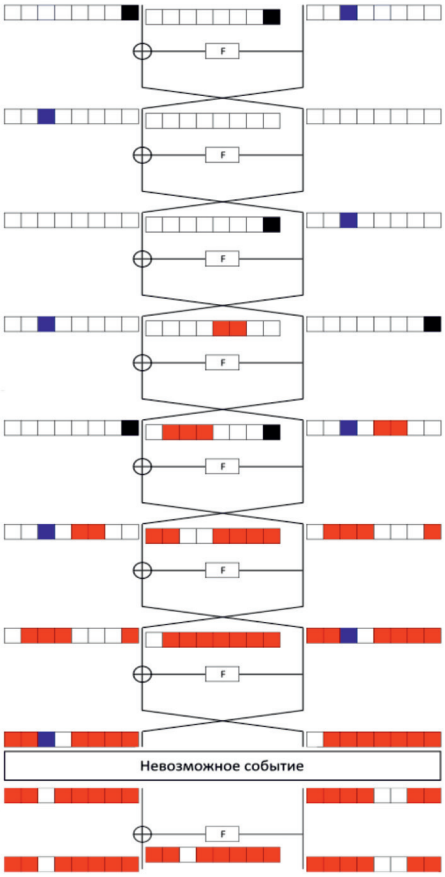

Рис. 5. Схема для восьми раундов

В результате эксперимента было показано, что метод работает и позволяет отбрасывать неверные значения для той части подключа, которая приходится на первый полубайт текста. Также показано, что увеличение количества текстов после определенного порога, зависящего от ключа, не увеличивает количество отбрасываемых вариантов подключей. Среднее время поиска части подключа по результатам работы программы было 4,34 секунды, а количество ключей, которое отбрасывалось в большинстве случаев, составило 8 из 16. Небольшая выборка экспериментальных данных приведена в табл. 2.

Так как при анализе отбрасываются варианты только первого полубайта ключа, необходимо провести анализ для остальных полубайтов ключа, что требует дальнейшего развития данного направления анализа, составление по аналогии схем для остальных полубайтов и проведение экспериментов. Также необходимо совершенствовать технику анализа с тем, чтобы попытаться увеличить количество раундов шифрования и заменить операцию побитового сложения по модулю 2 на операцию сложения 2^{32}. Это приведет к уменьшению вероятности поиска правильных текстов за счет свойства операции сложения по модулю 2^{32}, обратно пропорционально количеству ненулевых битов в рассматриваемом полубайте разности.

Работа выполнена при поддержке гранта РФФИ № 15-37-20007-мол-а-вед.

Список литературы

1. Бабенко Л.К. Ищукова Е.А. Сидоров И.Д. Параллельные алгоритмы для решения задач защиты информации. – М.: Горячая линия Телеком, 2014. – 304 с.

2. Ищукова Е.А., Калмыков И.А. Дифференциальные свойства S-блоков замены для алгоритма ГОСТ 28147-89 // Инженерный вестник Дона. – 2015. – № 4; URL: ivdon.ru/ru/magazine/archive/n4y2015/3284.

3. Ищукова Е.А. Разработка и исследование алгоритмов анализа стойкости блочных шифров методом дифференциального криптоанализа // Диссертация на соискание ученой степени кандидата технических наук. – Таганрог, 2007. – 207 с.

4. Криптографическая защита информации. Блочные шифры; URL: https://www.tc26.ru/standard/draft/

5. Biham E., Biryukov A., Shamir A. Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials // Advances in Cryptology – EUROCRYPT ‘99. Prague: Springer-Verlag. P. 12–23.

6. Biham E., Biryukov A., Shamir A. Miss in the Middle Attacks on IDEA, Khufu, and Khafre // 6th International Workshop on Fast Software Encryption (FSE 1999). Rome: Springer-Verlag. P. 124–138.

7. Lu J., Dunkelman O., Keller N., Kim J. New impossible differential attacks on AES // Progress in Cryptology – INDOCRYPT 2008. – Volume 5365 of the series Lecture Notes in Computer Science. – P. 279–293; http://link.springer.com/chapter/10.1007/978-3-540-89754-5_22.