УДК 004.056.55

АЛГОРИТМ ШИФРОВАНИЯ МАГМА: ОЦЕНКА КРИПТОСТОЙКОСТИ ШИФРА С ИСПОЛЬЗОВАНИЕМ ЛИНЕЙНОГО И СЛАЙДОВОГО МЕТОДОВ АНАЛИЗА

Алексеев Д.М.

Научный руководитель: к.т.н., доцент кафедры БИТ Ищукова Е.А.
Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, Таганрог, e-mail: alekseev_1994dima@mail.ru

В рамках данной работы разработаны, программно реализованы и протестированы параллельные алгоритмы поиска слайдовых пар текстов для шифра Магма для случаев циклически повторяющихся раундовых подключей. Рассмотрены случаи самоподобия в одном и двух раундах шифрования. В ходе проведенных исследований на основе использования метода слайдовой атаки получены обширные экспериментальные данные, отражающие зависимость скорости вычислений при поиске слайдовых пар текстов и ключа шифрования от используемого числа вычислительных узлов, параметров исследуемого шифра, способа межпроцессорного распределения данных. В данной статье представлено применение метода линейного криптоанализа к упрощенному алгоритму шифрования Магма. В результате работы проведен анализ блоков замены шифра и построены линейные статистические аналоги и соответствующие им вероятности.

Ключевые слова: криптография, криптоанализ, слайдовая атака, линейный анализ, секретный ключ, блочный алгоритм шифрования, симметричный шифр, Магма, стандарт шифрования РФ, ГОСТ Р 34.12-2015, параллельные вычисления, MPI

MAGMA ALGORITHM OF ENCRYPTION: ESTIMATION OF CIPHER CRYPTOGRAPHIC STRENGTH USING LINEAR AND SLIDE ANALYSIS METHODS

Alekseev D.M.

Scientific advisor: Candidate of Technical Sciences, Associate professor Ishchukova E.A.
Southern Federal University, Institute of Computer Technologies and Information Security, Taganrog, e-mail: alekseev_1994dima@mail.ru

In this work there were developed, software-implemented and tested out parallel algorithms of searching slide pairs of texts for Magma cipher in the case of periodically repeated round subkeys. Cases of self-similarity in one and two encryption cycles are examined. As a part of the study extensive experimental data based on the method of slide attack were obtained. These data show the interaction between computing speed in slide pairs of texts, cipher key and the number of computation nodes, cipher characteristics, methods of interprocess data distribution. This article presents the application of the method of linear cryptanalysis to the simplified linear cryptanalysis algorithm Magma. In the result of the study the analysis of the replacement blocks cipher is made, linear statistical analogs and their corresponding probabilities are constructed.

Keywords: Cryptography, cryptanalysis, slide attack, linear analysis, secret key, block encryption algorithm, symmetric cipher, Magma, encryption standard RF, GOST R 34.12-2015, parallel computing, MPI

С 2016 года в Российской Федерации вступил в силу новый криптографический стандарт ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» [1, с. 2]. В его состав вошли два алгоритма шифрования: ранее действовавший стандарт шифрования ГОСТ 28147-89 (переименован в «Магма») и новый блочный алгоритм шифрования Кузнечик.

Магма представляет собой симметричный блочный алгоритм шифрования с размером блока входных данных 64 бита, секретным ключом 256 бит и 32 раундами шифрования.

Линейный метод анализа

В связи с тем, что шифр Магма вошел в состав нового стандарта шифрования, его анализ является актуальной задачей. Исходя из того, что шифр Магма имеет фиксированные блоки замены (таблицы перестановок), его анализ с точки зрения линейного метода криптоанализа является актуальным.

Метод линейного криптоанализа впервые предложен в начале 90-х годов XX века японским ученым М. Матсуи и основывается на том, что существует возможность замены нелинейной функции ее линейным аналогом.

Ранее был проведен анализ блоков замены для алгоритма шифрования Магма. С результатами анализа можно ознакомиться в работе [2]. В ней показано, как, используя линейные свойства S-блоков замены, строить статистические аналоги для одного раунда шифрования. В результате, для первого блока замены для пары векторов

(α, β) = (1101, 0001), получим линейный статистический аналог:

$$X_{33} \oplus X_{34} \oplus X_{36} \oplus Y_{25} = K_1 \oplus K_2 \oplus K_4, \quad (1)$$

для которого вероятность того, что Q = 0, равна 0,25.

Однако для проведения анализа алгоритма шифрования этого не достаточно, так как во всех аналогах в левой части присутствуют неизвестные элементы, а именно значения *Y*.

Аналоги, пригодные для анализа, не должны содержать в себе неизвестных битов, кроме битов секретного ключа, которые необходимо найти в результате анализа. В связи с этим необходимо разработать механизмы, которые бы позволили объединить несколько линейных аналогов в один, исключив при этом биты, которые мешают проведению анализа.

Рассмотрим один из вариантов объединения линейных аналогов. Для этого возьмем линейный аналог, полученный для первого раунда шифрования. В нем присутствует бит Y_{25}. Обратимся к рис. 1, из которого видно, что сообщение Y^1 можно получить, сложив по модулю два левую часть входного сообщения X и сообщение B, поступающее на вход функции *F* второго раунда шифрования. Таким образом, бит Y_{25} можно представить как:

$$Y_{25}^1 = X_{25} \oplus B_{25}. \quad (2)$$

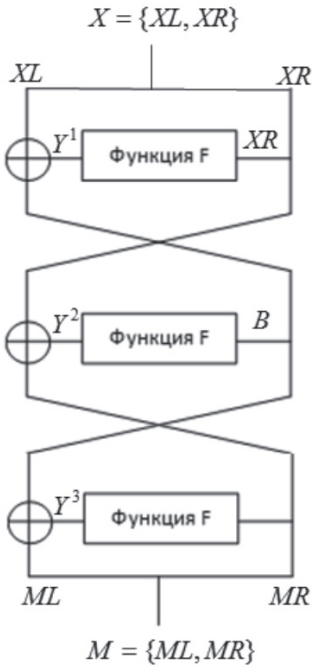

Рис. 1. Обозначения входов и выходов трех раундов шифра Магма

Теперь обратимся к третьему раунду шифрования и построим еще один линейный аналог с использованием той же пары векторов (α, β) = (1101, 0001), которая была использована для построения первого аналога. Для этого подробно рассмотрим прохождение битов сообщения через функцию *F* третьего раунда шифрования (рис. 2).

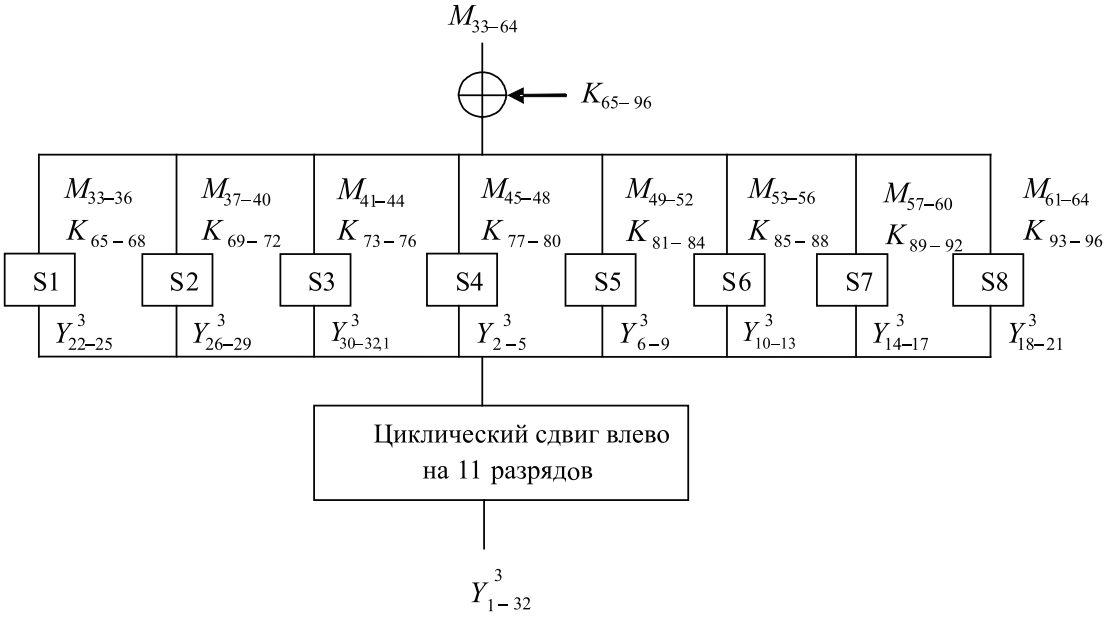

Рис. 2. Функция F для третьего раунда шифрования

Рассмотрим третий раунд шифрования. На вход функции F третьего раунда шифрования поступает 32-х битовая правая часть выходного сообщения $M_{33–64}$. Последовательность $M_{33–64}$ складывается по модулю 2 с третьим раундовым подключом $K_{65–96}$ (в соответствии с принципом выработки раундовых подключей для шифра Магма третий подключ содержит 65–96 биты исходного секретного ключа K). После сложения с подключом данные разбиваются на группы по 4 бита и поступают на вход соответствующих блоков замены. На рис. 2 показано побитовое представление данных при их прохождении через функцию F третьего раунда шифрования.

Для того, чтобы определить, какие биты будут получены на выходе каждого из блоков замены, необходимо к последовательности $Y^3_{1–32}$ применить операцию циклического сдвига вправо на 11 разрядов.

После того, как получено внутренне представление битов, можно перейти легко построить линейный статистический аналог для первого блока замены, определенный парой векторов $(\alpha,\beta)=(1101,0001)$:

$$M_{33} \oplus M_{34} \oplus M_{36} \oplus Y^3_{25} = K_{65} \oplus K_{66} \oplus K_{68}, \quad (3)$$

для которого вероятность того, что Q = 0, равна 0,25.

В последнем линейном аналоге присутствует бит Y^3_{25}. Обратимся к рис. 1, из которого можно видеть, что сообщение Y^3 можно получить, сложив по модулю два левую часть выходного сообщения Y и сообщение B, поступающее на вход функции F второго раунда шифрования. Таким образом, бит Y^3_{25} можно представить как:

$$Y^3_{25} = M_{25} \oplus B_{25}. \quad (4)$$

Путем сложения можем объединить аналоги (1) и (3):

$$X_{33} \oplus X_{34} \oplus X_{36} \oplus Y_{25} \oplus M_{33} \oplus M_{34} \oplus M_{36} \oplus Y^3_{25} = K_1 \oplus K_2 \oplus K_4 \oplus K_{65} \oplus K_{66} \oplus K_{68}. \quad (5)$$

Подставив в формулу (5) формулы (2) и (4), получим:

$$X_{33} \oplus X_{34} \oplus X_{36} \oplus X_{25} \oplus B_{25} \oplus M_{33} \oplus M_{34} \oplus M_{36} \oplus M_{25} \oplus B_{25} =$$

$$= K_1 \oplus K_2 \oplus K_4 \oplus K_{65} \oplus \oplus K_{66} \oplus K_{68}. \quad (6)$$

В результате такого объединения двух аналогов, а также в результате представления значений на выходах функций F (значения Y_i) в виде суммы по модулю два соответствующих входных (биты X_i) или выходных (биты Y_i) значений и значения на входе второго раунда шифрования (значения B_i) мы получили линейный статистический аналог (7), в котором неизвестными переменными являются только биты секретного ключа.

$$X_{33} \oplus X_{34} \oplus X_{36} \oplus X_{25} \oplus M_{33} \oplus M_{34} \oplus M_{36} \oplus M_{25} = K_1 \oplus K_2 \oplus K_4 \oplus K_{65} \oplus K_{66} \oplus K_{68} \quad (7)$$

В рамках исследования рассмотрен только первый этап линейного криптоанализа – анализ блоков замены и построение уравнений для одного и трех раундов шифрования. Дальнейшие исследования в области линейного анализа шифра Магма связаны с построением линейных статистических аналогов применительно к большему числу раундов алгоритма шифрования, а затем применение полученных данных к анализу полного шифра.

Слайдовый метод анализа

Метод слайдовой атаки впервые был предложен А. Бирюковым и Д. Вагнером [3, с. 245; 4, с. 589] и основан на гомогенности рассматриваемого шифра. Идея заключается в том, что можно сопоставить один процесс зашифрования с другим таким образом, что один из процессов будет «отставать» от другого на один раунд (или несколько раундов). Подробнее о применении слайдовой атаки можно прочесть в работе [5, с. 43].

Слайдовая атака с одним раундовым подключом

В ходе исследования была рассмотрена задача поиска слайдовой пары для случая, когда в алгоритме шифрования Магма используется один и тот же раундовый подключ, что возможно, так как в Магме отсутствует функция выработки раундовых подключей. Идея заключается в том, что можно сопоставить один процесс зашифрования с другим таким образом, что один из процессов будет «отставать» от другого на один раунд. Для Магмы это теоретически возможно в 2^{32} случаях из 2^{256}, когда для за-

шифрования данных будет использоваться один и тот же раундовый подключ. Поиск слайдовой пары путем полного перебора правой части парного текста представлен на рис. 3.

В результате был разработан и реализован алгоритм, состоящий из следующих шагов:

1. Зафиксировать один текст (входную 64-х битную последовательность) и левую часть парного текста, равную правой (исходной) части фиксированного текста.

2. Определить правую часть путем полного перебора ее возможных значений (от 0x00000000 до 0xffffffff).

3. Зашифровать фиксированный текст, а также парный текст (с перебираемой на текущем этапе правой частью).

4. Проверить критерий отбора слайдовых пар: левая часть шифр-текста, полученная для фиксированного текста, должна быть равна правой части шифр-текста, полученной для парного текста, в котором перебирается правая часть. Перейти к шагу 2.

5. После полного перебора правой части парного текста сформировать результат о поиске слайдовых пар.

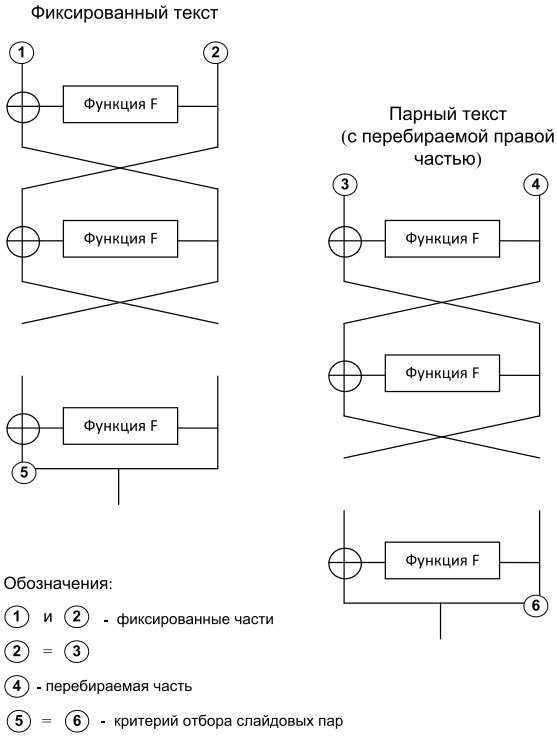

Рис. 3. Схема поиска слайдовой пары для одного подключа

Для проведения эксперимента в локальную сеть были объединены девять ЭВМ (каждая из которых использует для вычислений два ядра), после чего был протестирован разработанный алгоритм. Результаты измерений времени поиска слайдовых пар для каждого из процессов представлены в таблице.

Результаты измерений времени поиска слайдовых пар для разных процессов

Имя машины – номер процесса	Время поиска, с
01–0	2587,870496
01–9	2662,572554
03–1	2652,869916
03–10	2584,051360
04–2	2657,906713
04–11	2647,533539
05–3	2604,300599
05–12	2643,880999
06–4	2592,802551
06–13	2758,090014
11–5	2562,219539
11–14	2485,150132
12–6	2023,647694
12–15	1933,766277
13–7	4397,100301
13–16	3916,700942
14–8	2593,235726
14–17	2653,619990

Слайдовая атака с двумя раундовыми подключами

Также в ходе исследования была рассмотрена задача поиска слайдовой пары для случая, когда в алгоритме шифрования Магма циклически повторяются два раундовых подключа, при этом отсутствует смена порядка использования подключей в последних раундах шифрования. Таких комбинаций для различных значений двух ключей может быть 2^{64} от общего объема ключевого пространства 2^{256}.

Сопоставим два процесса шифрования друг с другом с отставанием на два раунда так, как показано на рис. 4.

Предполагается, что второй открытый текст X1 (XL1; XR1) является выходом второго раунда шифрования первого текста. Рассмотрим, как связаны между собой первый открытый текст X (XL, XR) и второй открытый текст X1 (XL1, XR1):

$$XR1 \oplus XL = F(XR, K1); \quad (8)$$

$$XL1 \oplus XR = F(XR1, K2). \quad (9)$$

K1 K2 K1 K2 K1 K2 . . . K1 K2

K1 K2 K1 K2 K1 K2 . . . K1 K2

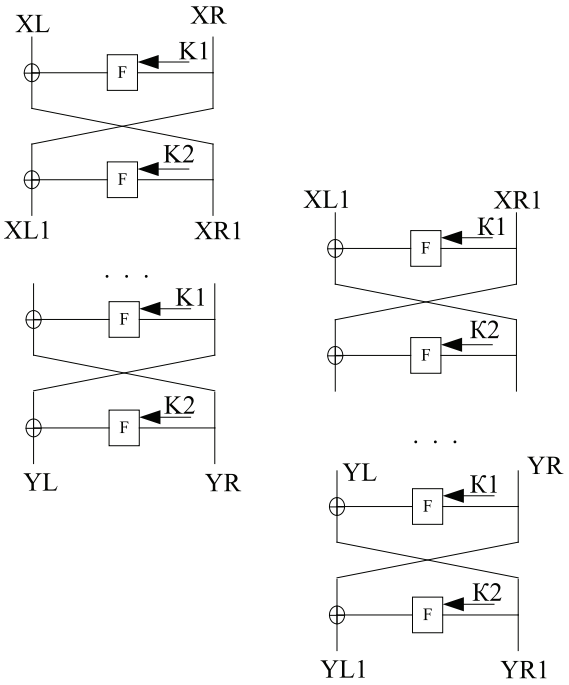

Рис. 4. Процесс шифрования с отставанием на два раунда

Аналогичным образом определим, как связаны между собой шифр-тексты *Y* (*YL*, *YR*) и *Y*1 (*YL*1, *YR*1) для первого и второго открытых текстов соответственно:

$$YL1 \oplus YR = F(YR1, K2); \quad (10)$$

$$YL \oplus YR1 = F(YR, K1). \quad (11)$$

В ходе исследований был разработан и реализован параллельный алгоритм поиска слайдовой пары и ключа шифрования, состоящий из следующих шагов:

1. Зафиксировать один текст (входную 64-х битную последовательность) X (XL; XR) и получить соответствующий ему шифр-текст *Y* (*YL*; *YR*).

2. Предположить второй текст X1 (XL1; XR1): зафиксировать левую часть текста XL1 и определить правую часть XR1 путем полного перебора ее возможных значений (от 0x00000000 до 0xffffffff). Если такой перебор полностью осуществлен, присвоить левой части текста XL1 новое значение.

3. Получить соответствующий шифр-текст *Y*1 (*YL*1; *YR*1) для второго текста X1 с перебираемой на текущем этапе правой частью.

4. Из формулы (8) вычислить значение первого подключа K1.

5. Подставить найденное значение первого подключа K1 в формулу (11). Если равенство не выполняется, то вернуться к шагу 2 и переопределить правую часть XR1 путем полного перебора ее возможных значений (от 0x00000000 до 0xffffffff).

6. Из формулы (9) вычислить значение второго подключа K2.

7. Подставить найденное значение второго подключа K2 в формулу (10). Если равенство не выполняется, то вернуться к шагу 2 и переопределить правую часть XR1 путем полного перебора ее возможных значений (от 0x00000000 до 0xffffffff).

8. Если оба равенства в формулах (11) и (10) выполняются, то найдена слайдовая пара и определен используемый секретный ключ.

Направление дальнейших исследований в области слайдовой атаки на шифр Магма связано с тестированием разработанного параллельного алгоритма для случая самоподобия подключей в двух ра-

ундах шифрования, а также разработкой алгоритма поиска слайдовых пар для 4-х однотипных подключей, а затем его применение к анализу полного шифра.

Исследования, представленные в данной работе, выполнены при поддержке гранта РФФИ №17-07-00654 А.

Список литературы

1. Криптографическая защита информации Блочные шифры // URL: https://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf.

2. Алексеев Д.М. Применение метода линейного криптоанализа к шифру Магма // Материалы VII Всероссийской молодежной школы-семинара по проблемам информационной безопасности «Перспектива-2016». – Таганрог: Изд-во ЮФУ, 2016. – С. 112-117.

3. Бирюков А., Вагнер Д. Слайдовые атаки // Труды быстрого программного шифрования. – 1999. – № 1636. – С. 245-259.

4. Бирюков А., Вагнер Д. Расширенная слайдовая атака. Достижения в криптологии // Еврокрипт. – 2000. – № 1807. – С. 589-606.

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