УДК 681.0.245

РАЗРАБОТКА АЛГОРИТМОВ ОЦЕНКИ СТОЙКОСТИ ПРОЕКТНОГО СТАНДАРТА ШИФРОВАНИЯ ГОСТ С ПОМОЩЬЮ МЕТОДА СЛАЙДОВОГО АНАЛИЗА

Ищукова Е.А.

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

В статье рассмотрена возможность применения метода слайдовой атаки к оценке стойкости алгоритмов шифрования, вошедших в проект нового стандарта шифрования данных в России, а именно: алгоритмов Магма и Кузнечик. Алгоритм Магма(бывший ГОСТ 28147089) построен по схеме Фейстеля, второй шифр Кузнечик представляет собой SP-сеть. В статье представлены алгоритмы поиска слайдовых пар текстов для алгоритма Магма в случае использования слабого секретного ключа. Рассмотрены случаи, когда в алгоритме используются ключи с одно-, двух- и четырехраундовым самоподобием. Для алгоритма Кузнечик также рассмотрены алгоритмы, направленные на анализ шифра с одно- и двухраундовым самоподобием. Приведенные алгоритмы и полученные с их использованием результаты не снижают практической стойкости рассматриваемых шифров. Однако могут быть использованы для дальнейшего всестороннего изучения симметричных блочных шифров, построенных как по принципу схемы Фейстеля, так и на основе SP-сети.

Ключевые слова: криптография, блочный шифр, Магма, ГОСТ 29147-89, Кузнечик, фиксированные блоки замены, слайдовая атака, слайдовая пара, самоподобие, схема Фейстеля, SP-сеть

DEVELOPMENT OF ALGORITHMS FOR THE ASSESSMENT OF RESISTANCE FOR ENCRYPTION STANDARD GOST USING THE METHOD SLIDE ATTACK

Ischukova E.A.

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

The article considers the possibility of using a slide attack to assessing the strenght of encryption algorithms included in the draft of a new Data Encryption Standard in Russia, namely algorithms Magma and Kuznechik. Magma algorithm (formerly GOST 28147089) was built under the scheme Feistel, another cipher Kuznechik is a SP-network. The paper presents algorithms for finding pairs of slide text for algorithm Magma in the case of a weak secret key. Consider the case where the algorithm used keys with one-, two- and four rounds self-similarity. For algorithm Kuznechik also considered algorithms aimed at the analysis of a cipher with one- and two- rounds self-similarity. These algorithms and results obtained with their help do not reduce the resistance of the practical consideration ciphers. However, there may be used for further comprehensive study symmetric block ciphers, constructed as a principle Feistel and SP-network.

Keywords: cryptography, block cipher, Magma, GOST 29147-89, Kuznechik, fixed replacement blocks, slide attack, slide couple, self-similarity, Fei9stel scheme, SP-network

С 1 января 2016 года в России в силу вступит новый криптографический стандарт ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» [5]. В его состав войдут два алгоритма шифрования: ныне действующий стандарт шифрования ГОСТ 28147-89 и новый блочный алгоритм шифрования Кузнечик. В составе нового стандарта действующий алгоритм шифрования ГОСТ 28147-89 именуется как Магма.

В настоящей статье предлагается рассмотреть возможные походы к анализу этих двух шифров с использованием метода слайдового анализа. Слайдовая атака (SlideAttacks) была предложена в 1999 году Алексом Бирюковым и Дэвидом Вагнером [1]. Этот метод анализа применим ко всем алгоритмам блочного шифрования и не зависит от числа раундов шифрования. Алгоритм может обладать самоподобием за счет периодического использования секретного ключа, что возможно в случае использования слабой функции выработки раундовых подключей. Поэтому анализ составной части шифра, отвечающей за выработку раундовых подключей, является важной частью анализа. Основная идея слайдовой атаки заключается в том, что можно сопоставить один процесс зашифрования с другим таким образом, что один из процессов будет «отставать» от другого на один раунд. Тогда, в случае успешного нахождения такой пары текстов, можно извлечь информацию о битах секретного ключа, проанализировав первый и последний раунды шифрования. Подробнее о применении слайдовой атаки можно прочесть в работе [1–4].

Так как для алгоритма Магма (n = 64) не предусмотрена функция выработки раундовых подключей, то мы предлагаем рассмотреть варианты, которые будут значительным образом ослаблять стойкость этого алгоритма. Рассмотрим случай, когда в алгоритме Магма все восемь раундовых подключей примут одно и то

же значение. Так как один раундовый подключ имеет длину 32 бита, то всего таких комбинаций для различных значений секретного ключа может быть 2^{32} от общего объема ключевого пространства 2^{256}. При такой длине ключа перебор всех комбинаций ключевого пространства составит всего 2^{32}. А при применении слайдовой атаки это значение может сократится до 2^{16} с ожиданием успеха p = 0,5 согласно парадоксу Дней Рождений.

Сопоставим два процесса зашифрования друг против друга с запаздыванием на один раунд так, как показано на рис. 1.

Так как алгоритм Магма построен по схеме Фейстеля, а мы предполагаем, что второй открытый текст является выходом первого раунда шифрования первого текста, то получаем следующий критерий отбора: XL1 = XR;YR1 = YL.

Алгоритм поиска слайдовой пары будет сводиться к следующим действиям:

Алгоритм 1

1. Зафиксировать первый текст X и соответствующий ему шифр Y.

2. Зафиксировать левую часть второго текста XL1 = XR.

3. Предположить правую часть второго текста XR1.

4. Получить шифр Y1

5. Если YR1 = YL, то вычислить ключ, иначе вернуться к шагу 3.

Так как перебор значений ведется только по правой половине блока XR1, которая может принимать одно из 2^{32} значений, то согласно парадоксу Дней Рождений, нам будет достаточно перебрать 2^{16} текстов для того, чтобы найти слайдовую пару с вероятностью успеха p = 0,5. Важно отметить, что эта и последующие рассматриваемые атаки будут работать при любом заполнении S-блоков, в том числе и для блоков, утвержденных для алгоритма Магма.

Теперь рассмотрим случай, когда в алгоритме Магма циклически повторяются два раундовых подключа и не меняют порядок следования в последних раундах шифрования.Это начальное допущение легко позволит выполнить слайдовую атаку. Но при этом важно помнить, что в оригинальном шифре Магма раундовые подключи меняют свой порядок следования. Таких комбинаций для различных значений двух ключей может быть 2^{64} от общего объема ключевого пространства 2^{256}. При такой длине ключа перебор всех комбинаций составит всего 2^{64}. А при применении слайдовой атаки это значение сократится до 2^{32}.

Сопоставим два процесса зашифрования друг против друга с запаздыванием на два раунда так, как показано на рис. 2. В этом случае мы предполагаем, что второй открытый текст является выходом второго раунда шифрования первого текста. Рассмотрим, как связаны между собой первый открытый текст (XL, XR) и второй открытый текст (XL1, XR1):

$$XR \oplus XL1 = F(XR, K1); \quad (1)$$

$$XL1 \oplus XR = F(XR1, K2); \quad (2)$$

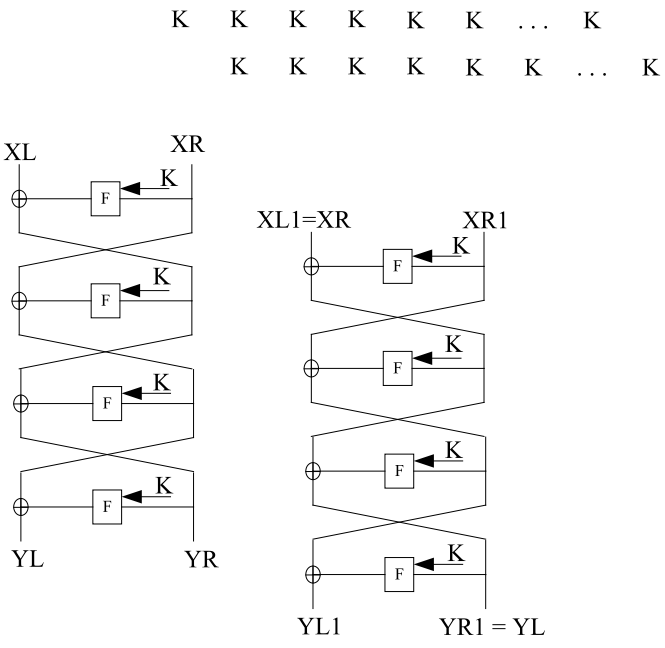

Рис. 1. Анализ шифра Магма с запаздыванием на 1 раунд

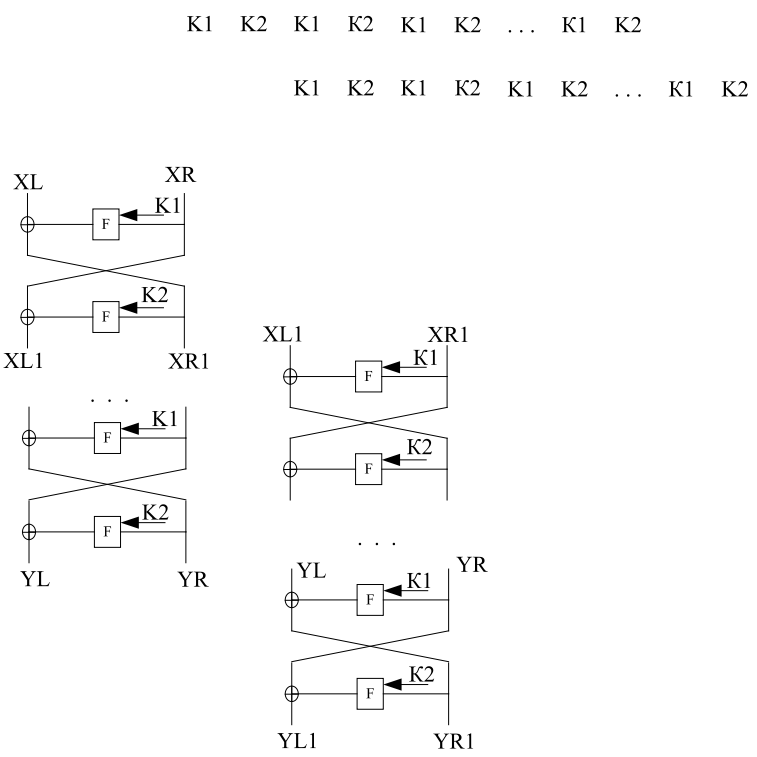

Рис. 2. Анализ шифра Магма с запаздыванием на 2 раунда

Аналогичным образом определим, как связаны между собой шифры для первого (YL, YR) и второго текстов (YL1, YR1):

$$YL1 \oplus YR = F(YR1, K2); \quad (3)$$

$$YL \oplus YR1 = F(YR, K1). \quad (4)$$

Алгоритм поиска слайдовой пары с одновременным нахождением ключа будет сводиться к следующим действиям:

Алгоритм 2

1. Зафиксировать первый текст X и соответствующий ему шифр Y.
2. Предположить второй текст X1 и получить соответствующий ему шифр Y1.
3. Из формулы (1) вычислить значение K1.
4. Подставить найденное значение в формулу (4). Если равенство не выполняется, то вернуться к шагу 2.
5. Из формулы (2) вычислить значение K2.
6. Подставить найденное значение в формулу (3). Если равенство не выполняется, то вернуться к шагу 2.
7. Если оба равенства в формулах (4) и (3) выполняются, то мы нашли слайдовую пару и определили используемый секретный ключ.

Согласно парадоксу Дней Рождений, нам будет достаточно перебрать 2^{32} текстов для того, чтобы найти слайдовую пару с вероятностью успеха p = 0,5.

Теперь рассмотрим случай, когда в алгоритме ГОСТ циклически повторяются четыре раундовых подключа K1 – K4 и не меняют порядок следования в последних раундах шифрования. Таких комбинаций для различных значений двух ключей может быть 2^{128} от общего объема ключевого пространства 2^{256}. При такой длине ключа перебор всех комбинаций составит всего 2^{128}. А при применении слайдовой атаки это значение сократится до 2^{65}.

Сопоставим два процесса зашифрования друг против друга с запаздыванием на четыре раунда так, как показано на рис. 3.

На рис. 3 показаны слева первые четыре раунда для преобразования первого текста и справа четыре последних раунда для преобразования второго текста. Также рис. 3 отражает взаимосвязь между первым открытым текстом (XL, XR) и вторым открытым текстом (XL1, XR1), а также между первым шифром (YL, YR) и вторым (YL1, YR1). На рис. 3 введены промежуточные значения A, B, C, D, которые отражают входы, поступающие на функцию F для второго и третьего раундов. В соответствии с рис. 3 можно выявить следующие связи для промежуточных значений:

$$A = XL \oplus F(XR, K1); \quad (5)$$

$$B = XR1 \oplus F(XL1, K4); \quad (6)$$

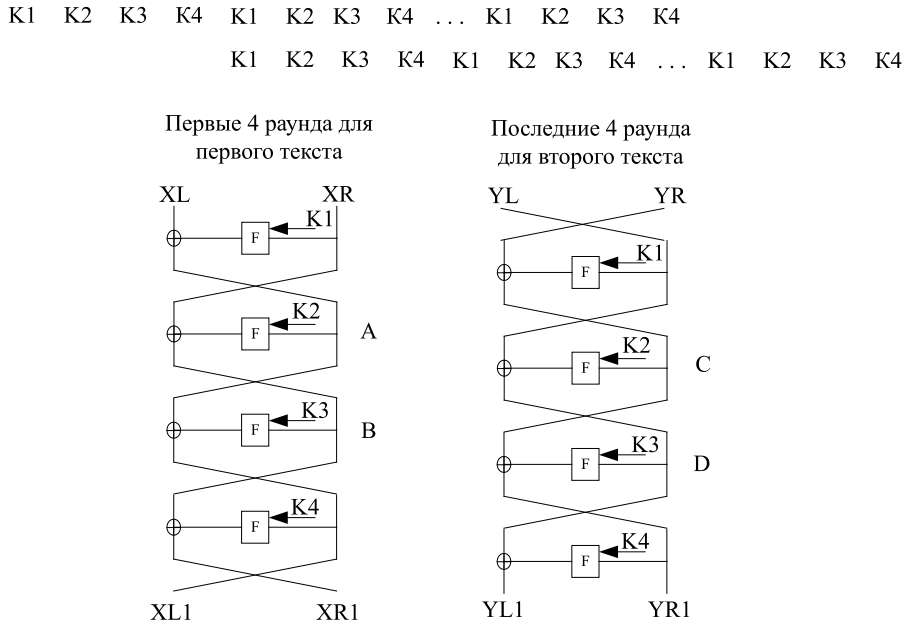

Рис. 3. Анализ шифра Магма с запаздыванием на 4 раунда

$$C = YR \oplus F(YL, K1); \quad (7)$$

$$D = YL1 \oplus F(YR1, K4); \quad (8)$$

$$A \oplus XL1 = F(B, K3); \quad (9)$$

$$C \oplus YR1 = F(D, K3). \quad (10)$$

Алгоритм будет заключаться в следующем. Для каждой потенциальной слайдовой пары мы будем строить таблицы для всех возможных значений K1 и для всех возможных значений K4. Итого две таблицы по 2^{32} значений каждая. Пробегая по таблицам будем смотреть, даст ли какая-нибудь комбинация K1 и K4 такие значения A, B, C, D, что будут выполнены равенства (9) и (10). Если равенства (9) и (10) будут выполнены, то это даст нам информацию о значениях ключей K1 и K2. Отсюда легко можно будет найти значение подключей K3 и K4. Согласно парадоксу Дней Рождений, нам будет достаточно перебрать 2^{32} текстов для того, чтобы найти слайдовую пару с вероятностью успеха p = 0,5. При этом для каждой потенциальной слайдовой пары необходимо будет сделать 2^{33} опробований (2 таблицы по 2^{32}). Таким образом, общая сложность анализа составит 2^{65} опробований.

Алгоритм поиска слайдовой пары с одновременным нахождением подключей будет сводиться к следующим действиям:

Алгоритм 3

1. Зафиксировать первый текст X и соответствующий ему шифр Y.

2. Предположить второй текст X1 и получить соответствующий ему шифр Y1.

3. Из формул (5) и (6) вычислить значения A и B для всех значений K1.

4. Из формул (7) и (8) вычислить значения C и D для всех значений K4.

5. Для всех значений (A, B) предположить значение K3 из формулы (9).

6. Для всех значений (C, D) предположить значение K3 из формулы (10).

7. Если значения K3 из п. 5 не совпадают со значениями K3 из п.6, то вернуться к шагу 2.

8. Из найденных значений K1, K2, K3 вычислить раундовый подключ K4.

Теперь рассмотрим вариант применения слайдовой атаки к анализу алгоритма Кузнечик. Для этого прежде всего оговорим рассматриваемые допущения. В алгоритме Кузнечик используется функция выработки раундовых подключей, построенная по схеме Фейстеля. Основываясь на этом, для оригинального шифра можно показать, что единственно потенциально возможным случаем повторения раундовых подключей является вариант, когда ключи будут циклически повторяться 1 по 5. Остальные варианты выработки одинаковых циклических ключей невозможны. Тем не менее мы рассмотрим случаи для вариантов Кузнечика с повторяющимися раундовыми ключами с тем, чтобы в дальнейшем можно было понять, как перейти от простых вариантов анализа к более сложным. В случае с одним, циклически повторяющимся раундовым ключом, сопоставим два процесса зашифрования с запаздыванием на один раунд так, как показано на рис. 4. Тогда вы-

ход первого раунда зашифрования первого текста X будет являться входным значением X1 второго процесса зашифрования. Точно также выходное зашифрованное значение Y будет являться промежуточным значением второго процесса зашифрования перед последним преобразованием S. Рассмотрим условия поиска слайдовых пар. Для этого определим, каким соотношением должны быть связаны значения X1 и X. Согласно схеме, мы ожидаем, что X1 будет выходом первого раунда зашифрования значения X, тогда

$$X \oplus K1 = S^{-1}(L^{-1}(X1)). \quad (11)$$

Аналогичным образом рассмотрим, каким соотношением связаны значения выходов Y и Y1. Мы ожидаем, что значение Y поступает на вход последнего преобразования S. Тогда

$$Y1 \oplus K1 = L(S(Y)). \quad (12)$$

Из формул (11) и (12) получаем, что

$$K1 = X \oplus S^{-1}(L^{-1}(X1)), \quad (13)$$

$$K1 = Y1 \oplus L(S(Y)). \quad (14)$$

Так как в каждом раунде используется один и тот же раундовый подключ, то, объединив выражения (13) и (14), получаем условие отбора слайдовых пар

$$X \oplus S^{-1}(L^{-1}(X1)) = Y1 \oplus L(S(Y)) \quad (15)$$

Вопрос только в том, сколько текстов нам придется перебрать, прежде чем мы найдем хотя бы одну такую слайдовую пару. Согласно парадоксу Дней Рождений, при переборе 2^{64} разных текстов нас может ожидать успех с вероятностью p = 0,5.

Теперь рассмотрим случай, когда циклически повторяются два раундовых подключа (рис. 5). Необходимо сопоставить два процесса зашифрования, но с запаздыванием на два раунда. Тогда выход второго раунда зашифрования первого текста X будет являться входным значением X1 второго процесса зашифрования. Точно так же выходное зашифрованное значение Y будет являться промежуточным значением второго процесса зашифрования перед предпоследним преобразованием S. Рассмотрим условия поиска слайдовых пар. Для этого определим, каким соотношением должны быть связаны значения X1 и X. Согласно схеме, мы ожидаем, что X1 будет выходом второго раунда зашифрования значения X, тогда

$$X \oplus K1 = S^{-1}(L^{-1}(S^{-1}(L^{-1}(X1)) \oplus K2)). \quad (16)$$

Аналогичным образом рассмотрим, каким соотношением связаны значения выходов Y и Y1. Мы ожидаем, что значение Y поступает на вход предпоследнего преобразования S. Тогда

$$L(S(Y)) \oplus K1 = S^{-1}(L^{-1}(Y1 \oplus K2)). \quad (17)$$

Из формул (16) и (17) получаем, что

$$K1 = X \oplus S^{-1}(L^{-1}(S^{-1}(L^{-1}(X1)) \oplus K2)), \quad (18)$$

$$K1 = L(S(Y)) \oplus S^{-1}(L^{-1}(Y1 \oplus K2)). \quad (19)$$

Так как для обоих процессов зашифрования значение K1 будет одним и тем же, то, объединив выражения (8) и (9) получаем следующее соотношение:

$$X \oplus S^{-1}(L^{-1}(S^{-1}(L^{-1}(X1)) \oplus K2)) = L(S(Y)) \oplus S^{-1}(L^{-1}(Y1 \oplus K2)). \quad (20)$$

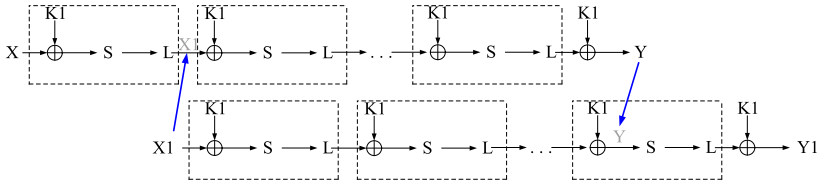

Рис. 4. Анализ шифра Кузнечик с запаздыванием на 1 раунд

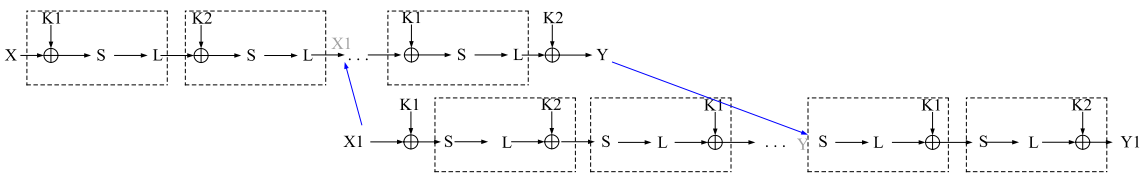

Рис. 5. Анализ шифра Кузнечик с запаздыванием на 2 раунда

В выражении (20) присутствует неизвестный нам ключ К2. Поэтому для каждой пары значений (X, Y); (X1, Y1) необходимо будет перебирать все возможные варианты ключа К2. Если равенство (20) выполнится, то это будет искомая слайдовая пара и ключ К2, а значение ключа К1 можно будет легко восстановить по формулам (18), (19). Согласно парадоксу Дней Рождений, для нахождения правильной слайдовой пары с вероятностью успеха $p = 0,5$, нам понадобится перебрать $2^{64}*2^{128} = 2^{192}$ различных текстов, что значительно меньше объема полного перебора 2^{256}.

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

Список литературы

1. Бабенко Л.К., Ищукова Е.А. «Анализ симметричных криптосистем» // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность». Таганрог: Изд-во ТТИ ЮФУ, 2012. – № 11. – С. 136–147.

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

3. Бабенко Л.К., Ищукова Е.А. «Современные алгоритмы шифрования и методы их анализа».Учебное пособие – Москва, «Гелиос АРВ», 2006.

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

5. Biryukov A., & Wagner D. (1999). Slide Attacks. Proceedings of Fast Software Encryption'99: Vol. 1636. Lecture Notes in Computer Science (P. 245–259). New York: Springer-Velgar.