DOI: 10.17117/na.2015.07.596

Поступило в редакцию: 17.07.2015

<http://ucom.ru/doc/na.2015.07.596.pdf>

Бабенко Л.К., Ищукова Е.А.
Применение слайдовой атаки для анализа
симметричных блочных шифров

Babenko L.K., Ischukova E.A.
The use of a slide attack to analyze of symmetric block cipher

В статье рассматриваются основные подходы к проведению анализа симметричных блочных шифров с использованием метода слайдового анализа. В том числе рассматриваются различные усовершенствованные метода анализа, такие как слайдовая атака с использованием дополнений, а также слайдовая атака с петлей.

Рассматривается пример практического применения данного вида анализа на упрощенной модели алгоритма шифрования DES

Ключевые слова: Криптография, криптоанализ, блочный шифр, секретный ключ шифрования, слайдовая атака, слайдовая атака с использованием дополнений, слайдовая атака с петлей

The article discusses the main approaches to the analysis of symmetric block cipher using the slide attack. Including discusses various advanced methods of analysis, such as the Complementation slide, as well as slide attack with a twist. An example of the practical application of this analysis type for a simplified model of the encryption algorithm DES is given

Key words: Cryptography, cryptanalysis, block cipher, a secret encryption key, slide attack, Complementation slide, slide attack with a twist

Бабенко Людмила Климентьевна

*Доктор технических наук, профессор
Южный федеральный университет
Ростовская обл., г. Таганрог, ул. Чехова, 2*

Babenko Ludmila Klimentievna

*Doctor of Engineering Sciences, Professor
Southern federal university
Rostov region, Taganrog, Chehov st., 2*

Ищукова Евгения Александровна

*Кандидат технических наук, доцент
Южный федеральный университет
Ростовская обл., г. Таганрог, ул. Чехова, 2*

Ischukova Evgeniya Alexandrovna

*Candidate of Engineering Sciences, Associate
Professor
Southern federal university
Rostov region, Taganrog, Chehov st., 2*

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

С ростом скорости современных компьютеров, скоростные алгоритмы шифрования используют все больше и больше раундов, признавая все существующие криптоаналитические технологии бесполезными. Это главным образом происходит из-за того, что такие популярные методы, как линейный и дифференциальный криптоанализ, являются статистическими атаками, превосходными при статистических непостоянствах. Однако, когда алгоритм

шифрования имеет большое количество раундов, каждый добавленный раунд к требует экспоненциального роста усилий атакующего.

Стремление к большому числу раундов можно наглядно увидеть, рассмотрев претендентов на конкурс AES. Несмотря на то, что одним из основных критериев для претендентов была скорость, некоторые представленные кандидаты (при этом не самые медленные) имели действительно большое число раундов: RC6(20), MARS(32), SERPENT(32), CAST(48). Это является следствием того, что после некоторого большого числа раундов даже относительно слабый шифр становится стойким. То же самое можно сказать и об отечественном стандарте шифрования данных ГОСТ 28147-89, 32 раунда которого призваны обеспечить достаточную стойкость даже при использовании потенциально уязвимых блоков замены.

В настоящей работе мы предлагаем рассмотреть метод криптоанализа, не зависящий от числа раундов в алгоритме шифрования, который называется “слайдовой атакой” или “скользящей атакой” (Slide Attacks). Данный метод анализа был предложен в 1999 году А. Бирюковым и Д. Вагнером [1, 2]. Этот метод применим ко всем алгоритмам блочного шифрования, но в большей степени он применим с тем шифром, которые обладают некоторой степенью гомогенности, то есть к тем шифрам, в которых одинаковые действия выполняются несколько раз.

В то время как два других метода криптоанализа, такие как линейный и дифференциальный, концентрируются главным образом на распространенных свойствах техники шифрования, слайдовая атака использует степень самоподобия, что является принципиальным отличием. Под самоподобием понимается использование одной и той же криптографической F-функции, зависящей от одного и того же подключа, в каждом раунде шифрования или циклически повторяясь через некоторое количество раундов. В зависимости от структуры алгоритма шифрования слайдовая атака может использовать как слабость процедуры формирования подключей, так и более общие структурные свойства шифра. Самый простой вид этой атаки обычно легко пресечь, избавившись от самоподобия в алгоритме шифрования. Более сложные варианты этой атаки имеют более сложный анализ, и против них гораздо труднее защититься.

Самый простой вариант слайдовой атаки рассчитан на анализ алгоритмов шифрования, состоящих из r раундов, каждый из которых содержит в себе F-функцию, зависящую от одного и того же значения ключа K . Такой тип алгоритмов шифрования называется гомогенным. К гомогенным также относятся алгоритмы, в которых функция формирования подключа периодична, то есть один и тот же подключ извлекается через равное количество раундов. Говоря математическим языком, $F_i = F_j$ для всех $i \equiv j \pmod{p}$, где p является периодом. В самом простом случае $p=1$, и в каждом раунде используется один и тот же подключ.

Рис. 1. Схема обычного блочного алгоритма шифрования

При рассмотрении слайдовых атак, с целью упрощения мы будем вначале рассматривать алгоритмы шифрования, в которых сложение шифруемых данных с подключом происходит непосредственно перед F -функцией. Так, если мы рассматриваем алгоритм шифрования, построенный по схеме Фейстеля, на вход которого поступает n -битное сообщение, то длина подключа будет составлять $n/2$ битов. На рис. 1 показан процесс зашифрования n -битового открытого текста X_0 , в результате которого получается шифр-текст X_r . Здесь X_j обозначает промежуточное значение данных после j -го раунда зашифрования, так что $X_j = F_j(X_{j-1}, k_j)$, где $j = 1, 2, 3 \dots r$. В дальнейшем мы иногда будем опускать значение k в обозначении F -функций, и будем писать $F(x)$ или $F_i(x)$ вместо $F(x, k)$ или $F_i(x, k)$.

Функция F называется слабой в том случае, если при известных двух равенствах $F(x_1, k) = y_1$ и $F(x_2, k) = y_2$ ключ k легко определяется. На рис. 2 показано, как может быть применена слайдовая атака к алгоритмам шифрования такого типа.

Рис. 2. Схема обычной слайдовой атаки

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.

Пусть X_0 и X_0' обозначают исходные открытые тексты, $X_j = F_j(X_{j-1})$ и $X_j' = F_j(X_{j-1}')$, где $j = 1, 2, 3 \dots r$. Идея заключается в том, что если мы имеем такую пару значений, что $X_1 = X_0'$, то мы также будем иметь соответствующую им пару значений, такую что $X_r = X_{r-1}'$. Предположим, что $X_j = X_{j-1}'$, тогда мы можем сказать, что $X_{j+1} = F(X_j) = F(X_{j-1}') = X_j'$. Пара открытых текстов и соответствующих им шифр-текстов (P, C) , (P', C') называется слайдовой парой в том случае, если $F(P) = P'$ и $F(C) = C'$.

Слайдовая атака проходит следующим образом. Мы получаем $2n/2$ пар открытый – закрытый текст (P_i, C_i) , и ищем среди них слайдовые пары. Согласно парадоксу дней рождений, мы ожидаем найти хотя бы одну пару индексов i, i' , такую, что $F(P_i) = P_{i'}$ и $F(C_i) = C_{i'}$ одновременно выполняются для некоторого ключа. После того, как слайдовая пара найдена, мы можем найти некоторые биты подключа. В том случае, если раундовая функция слабая, мы можем найти весь подключ данного раунда. Для нахождения оставшихся битов секретного ключа необходимо определить следующую слайдовую пару, и с ее по-

мощью провести анализ. Таким образом, достаточно найти всего несколько слайдовых пар для полного определения битов секретного ключа, что и является задачей, стоящей перед криптоаналитиком.

В случае, когда речь идет об алгоритмах шифрования, построенных по схеме Фейстеля, раундовая функция $F((l,r), k) = ((l \oplus f(r), r), k)$ модифицирует только половину входного сообщения. Таким образом, условие $F(x) = x'$ можно легко проверить с помощью сравнения левой части сообщения x и правой части сообщения x' . Это условие позволяет нам снизить сложность атаки на основе известных открытых текстов до $2^{n/2}$ известных текстов. У нас есть n -битовое условие нахождения потенциальной слайдовой пары: если (P_i, C_i) образует слайдовую пару вместе с (P_j', C_j') , то тогда $F(P_i) = P_j'$ и $F(C_i) = C_j'$. Для нахождения слайдовой пары для алгоритмов шифрования, построенных по схеме Фейстеля, необходимо известные тексты (P_i, C_i) занести в таблицу, после чего для каждого j найти такой текст, чтобы правые половины P_i и C_j' были равны левым половинам P_j' и C_i .

Если не все биты подключа будут найдены с помощью определенной слайдовой пары, то можно будет использовать другие слайдовые пары для определения оставшихся битов.

Для алгоритмов шифрования, построенных по схеме Фейстеля, сложность анализа может быть снижена до $2^{n/4}$ текстов в том случае, если существует возможность использовать выбранные открытые тексты. Для этого необходимо выбрать произвольным образом $n/2$ битовое значение x . После этого надо подобрать массив из $2^{n/4}$ открытых текстов $P_i = (x, u_i)$, которые будут различаться только случайно выбранной правой частью, и массив из $2^{n/4}$ текстов $P_j' = (u_j', x)$, которые будут различаться только случайно выбранной левой частью. Таким образом, у нас появится $2^{n/2}$ пар открытых текстов, и можно будет надеяться найти среди них хотя бы одну правильную пару.

Рис. 3. Слайдовая атака с использованием дополнений

Слайдовая атака с использованием дополнений (Complementation slide). Сначала рассмотрим метод, позволяющий анализировать алгоритм шифрова-

ния, построенный по схеме Фейстеля, с двухраундовым самоподобием (то есть когда в алгоритме используются два постоянно чередующихся подключа K_0 и K_1 , как показано на рис. 3).

При применении обычной слайдовой атаки к алгоритму с двухраундовым самоподобием логично было бы сопоставлять два процесса зашифрования с «запаздыванием» на два раунда, однако в этом случае атака является неэффективной.

Существует возможность сопоставить процессы зашифрования с «запаздыванием» на один раунд, если ввести разность $\Delta = K_0 \oplus K_1$ между двумя процессами зашифрования в каждом раунде. В этом случае мы переходим от двухраундового самоподобия к однораундовому самоподобию. Но вместе с этим, мы получаем разность между раундами зашифрования в слайдовых парах.

Для проведения атаки необходимо выбрать такую слайдовую пару, чтобы разность открытых текстов компенсировала разность подключей. Для этого необходимо найти открытые тексты, имеющие слайдовую разность (Δ, Δ) . Очевидно, что пара открытых текстов P и P' имеет слайдовую разность Δ в том случае, если $F(P) \oplus P' = \Delta$. Такая слайдовая разность будет переходить из раунда в раунд с вероятностью $p = 1$, и таким образом приведет к такой же разности шифр-текстов. На рис. 3 наглядно показано применение этого метода криптоанализа.

Как и в предыдущих случаях, слайдовая пара может быть выделена из массива, состоящего из $2n/2$ открытых текстов. Если мы обозначим открытый текст как $P = (L, R)$ и шифртекст как $C = (N, M)$. То получим следующие равенства:

$$\begin{aligned}(L', R') &= (R, L \oplus f(K_0 \oplus R)) \oplus (\Delta, \Delta); \\(N', M') &= (M \oplus f(K_1 \oplus N \oplus \Delta), N) \oplus (\Delta, \Delta).\end{aligned}$$

Из приведенных уравнений видно, что $L' = R \oplus \Delta$ и $M' = N \oplus \Delta$. Таким образом, получается, что $L' \oplus M' = R \oplus \Delta \oplus N \oplus \Delta = R \oplus N$, что и является $n/2$ -битовым условием определения слайдовой пары. Найденная слайдовая пара даст нам значения L, R, M, N, L', R', M' и N' . Так как известно, что $R = L \oplus \Delta$, то можно определить значение Δ : $\Delta = R \oplus L$. Сложив по модулю два значения $L \oplus \Delta \oplus R'$ получим значение на выходе функции F первого раунда шифрования первой слайдовой пары. Так как известны преобразования функции F и они не зависят от ключа, то можно предположить какое значение могло поступать на вход функции F первого раунда шифрования первой слайдовой пары. А так как мы знаем, что на вход этой функции поступает сумма значений $R \oplus K_0$, то это позволит нам предположить значение K_0 . Аналогичные действия необходимо провести с последним раундом шифрования второй слайдовой пары. Там на выходе функции F окажется сумма $M \oplus \Delta \oplus N'$. На вход же этой функции поступает значение $M' \oplus K_1$. А значит можно предположить возможные значения K_1 . Из предположенных ранее значений K_0 и K_1 верными будут те, сумма которых по модулю два даст значение Δ . Таким образом, главной задачей является нахождение правильной слайдовой пары, последующий же анализ не представляет особых трудностей и протекает довольно легко.

Слайдовая атака с петлей (Sliding with a Twist). Если не принимать во внимание начальную и конечную перестановки, часто используемые в алгоритмах блочного шифрования, то можно сказать, что для алгоритма шифрования, построенного по схеме Фейстеля, процесс дешифрования с использованием подключей K_0 , K_1 будет аналогичен процессу зашифрования с использованием подключей K_1 , K_0 . Также можно сказать, что процесс зашифрования с помощью алгоритмов, построенных по схеме Фейстеля, с использованием подключей K_0 , K_1 очень близок к процессу зашифрования тем же самым алгоритмом с использованием подключей K_1 , K_0 : просто один процесс «запаздывает» относительно другого на один раунд. Поэтому, можно сопоставить процессы зашифрования и дешифрования таким образом, что один из них будет «запаздывать» на один раунд. В этом случае слайдовые пары будут иметь частичное совпадение во всех раундах шифрования, за исключением первого раунда зашифрования и последнего раунда дешифрования. На рис. 4 показано, как необходимо сопоставить два этих процесса.

Рис. 4. Слайдовая атака с петлей

Криптоанализ начинается с создания массива из $2n/2$ открытых текстов, для того, чтобы можно было найти по крайней мере одну слайдовую пару. Для искомой слайдовой пары должны выполняться равенства:

$$\begin{aligned}(N', M') &= (R, L \oplus f(K_0 \oplus R)), \\ (L', R') &= (M \oplus f(K_0 \oplus N), N).\end{aligned}$$

Данные уравнения дают n -битовое условие отбора слайдовой пары (то есть $N' = R$ и $R' = N$). Найдя слайдовую пару, легко можно определить биты под ключа K_0 тем же способом, который был описан выше. Подключ K_1 может быть получен путем слайдовой атаки с «запаздыванием» на два раунда шифрования. При этом для анализа можно использовать ранее созданный массив текстов.

Существует также возможность проводить атаку на основе выборочных пар открытый – закрытый текст. В этом случае число требуемых текстов снижается до $2n/4$. При этом необходимо сгенерировать массив из $2n/4$ открытых текстов (L_i, R), имеющих различие только в левой половине текста, и получить соответствующие им значения шифртекстов. Так же необходимо сгенерировать массив из $2n/4$ шифртекстов текстов (M_j', N'), где $N' = R$, где имеются различия только в левой половине текста, и получить соответствующие им значения открытых текстов. Имея такое количество открытых текстов и шифртекстов, мы можем найти как минимум одну слайдовую пару. Дальнейший анализ будет аналогичен предыдущему.

На практике часто приходится пользоваться ни каким-либо одним методом анализа, а комбинацией методов, позволяющей достичь цели с минимальными затратами. Рассмотрим анализ алгоритма шифрования, построенного по схеме Фейстеля, с четырехраундовым самоподобием (4K-Feistel шифр), основанный на комбинации методов слайдовой атаки с использованием дополнений и слайдовой атаки с петлей.

Конечно, существует вариант, когда можно просто сопоставить процессы зашифрования с «запаздыванием» на два раунда следующим образом:

K0	K1	K2	K3	K0	K1...
K0	K1	K2	K3	K0	K1...

А после этого применить слайдовую атаку с использованием дополнений ($K1 \oplus K3, K0 \oplus K2$). Однако для проведения такого анализа требуется никак не меньше $2n/2$ текстов, да и сам процесс анализа довольно трудоемок [2].

Лучшего результата можно достигнуть, применив слайдовую атаку с петлей. Этот метод атаки применим в том случае, если одновременно объединить его со слайдовой атакой с использованием дополнений следующим образом:

K0	K1	K2	K3	K0	K1	K2	K3	K0...
K3	K2	K1	K0	K3	K2	K1	K0	K3...

Здесь верхний ряд соответствует процессу зашифрования, а нижний – процессу дешифрования (или процессу зашифрования с последовательным использованием подключей K3, K2, K1 и K0).

Теперь можно заметить, что появилась возможность применения слайдовой атаки с использованием дополнений, если есть возможность получить тексты, имеющие слайдовую разность $(0, K1 \oplus K3)$. Как видно из рис. 5 такой выбор разностей между слайдовыми парами обусловлен тем, что во втором раунде шифрования первой слайдовой пары, а также в предпоследнем раунде шифрования второй слайдовой пары используется подключ K1, в то время как в первом раунде шифрования второй слайдовой пары и в последнем раунде первой слайдовой пары используется подключ K3.

Такой подход к анализу алгоритма позволит определить значение подключа K0, а также значение Δ , позволяющее предположить значения подключей K1 и K3. В любом случае выбранный криптоаналитиком метод для анализа требует от него творческого подхода и фундаментальных знаний.

Для того чтобы убедиться на практике в действенности метода слайдовой атаки, рассмотрим ее применение к алгоритму шифрования S-DES. Алгоритм S-DES был разработан в учебных целях и имеет DES-подобную структуру, повторяя в своем составе преобразования, аналогичные преобразованиям алгоритма DES, но оперирующие с небольшими блоками данных. Алгоритм S-DES преобразует блок открытого текста блочной 8 бит под воздействием 10-битного секретного ключа. Подробное описание работы алгоритма S-DES можно найти в работе [3]. Так как алгоритм S-DES является блочным алгоритмом шифрования, построенном по схеме Фейстеля, то к нему вполне можно применить анализ на основе выборочного открытого текста. Для простоты работы будем использовать один и тот же фиксированный 8-ми битовый ключ K (то есть будем опускать процедуру получения 8-ми битового подключа из исходного 10-битового). Но при этом сложение шифруемых данных с ключом будет происходить не перед F-функцией, а непосредственно в ней, как это и предусмотрено алгоритмом. Также, мы опустим начальную и конечную перестановки, так как они не влияют на криптографическую стойкость алгоритма. И будем использовать не 2 цикла криптографического преобразования, а 20.

Сначала выберем произвольным образом 4-битовое значение x . Пусть $x = 1101$. После этого подберем массив из $2^{n/4} = 2^{8/4} = 2^2 = 4$ открытых текстов $P_i = (x=X_L, y_i=X_R)$, которые будут различаться только случайно выбранной правой частью, и массив из $2^{n/4} = 2^{8/4} = 2^2 = 4$ открытых текстов $P_j' = (y_j'=X_L', x=X_R')$, которые будут различаться только случайно выбранной левой частью. После этого зашифруем выбранные тексты на случайно выбранном 8-битовом ключе $K=(K1, K2)$, состоящем из двух 4-битовых частей (каждая из которых влияет на вход S-блока). Результаты зашифрования массивов $P_i = (x, y_i)$ и $P_j' = (y_j', x)$ приведены соответственно в табл. 1 и 2.

Таблица 1. Результаты зашифрования массива $P_i = (x, y_i)$ на секретном ключе K

№	X_L	X_R	Y_L	Y_R
1	1101	0110	0101	1100
2	1101	0001	1101	1110
3	1101	0010	1001	1010
4	1101	1000	0000	0111

Таблица 2. Результаты зашифрования массива $P_j' = (y_j', x)$ на секретном ключе K

№	X_L'	X_R'	Y_L'	Y_R'
1	1010	1101	1010	1101
2	0010	1101	0101	1111
3	1110	1101	1100	1000
4	1100	1101	0000	0011

Итак, есть 16 пар открытых текстов. Проанализировав результаты шифрования, приведенные в табл. 1 и 2, можно определить, что условию определения слайдовых пар удовлетворяют две пары текстов.

Так как при анализе найденных пар придется работать с таблицами замены, используемыми в алгоритме шифрования S-DES, то для удобства работы мы сопоставили входы и выходы блоков так, как показано в табл. 3.

Таблица 3. Соответствие входов и выходов S-блоков для алгоритма шифрования S-DES

Вход в S блок	Выход S0 блока	Выход S1 блока
0000	01	01
0001	11	10
0010	00	01
0011	10	00
0100	11	10
0101	01	01
0110	10	11
0111	00	11
1000	00	11
1001	11	10
1010	10	00
1011	01	01
1100	01	01
1101	11	00
1110	11	00
1111	01	11

Первую пару текстов составляют текст №1 в табл. 1 и текст №3 в табл. 2. Проанализируем найденную слайдовую пару. Для этого рассмотрим первые два раунда шифрования, показанные на рис. 6.

Рис. 6. Анализ первых раундов первой слайдовой пары

То, что известны значения X_R' и X_L , дает информацию о значении входа $F1'$ функции. Так как значения X_R и X_L' тоже известны, то легко можно определить значение выхода F-функции, которое будет равно 1000.

Так как перед выходом из F-функции данные подвергаются перестановке $P=(2,4,3,1)$, то, сделав шаг назад, можно определить, что на выходе S-блоков появляется значение 0100. То есть 01 является выходом S0 блока, а 00 – выходом S1 блока.

Входное сообщение F-функции подвергается перестановке с расширением $E/P=(4,1,2,3,2,3,4,1)$. А значит вход F-функции 1101 преобразуется к значению 11101011, которое и будет сложено с ключом $K=(K1, K2)$. То есть получается, что вход $S0$ блока $1110 \oplus K1$ даст на выходе значение 01, а вход $S1$ блока $1011 \oplus K2$ – значение 00.

Воспользовавшись табл. 3, можно определить, что значение 01 появляется на выходе $S0$ блока в случае, если на его вход поступило одно из следующих значений: 0000, 0101, 1011, 1100 или 1111. Таким образом, добавив к каждому из возможных значений входа значение 1110, получим возможные значения $K1$. Это будут значения 1110, 1011, 0101, 0010 или 0001. Аналогичным образом определяем, что значение 00 появляется на выходе $S1$ блока в случае, если на его вход поступило одно из следующих значений: 0011, 1010, 1101 или 1110. А значит, добавив к каждому из возможных значений входа значение 1011, получим возможные значения $K2$. Это будут значения 1000, 0001, 0110 или 0101. Теперь рассмотрим последние два раунда шифрования для этой же слайдовой пары, показанные на рис. 7.

Рис. 7. Анализ последних раундов первой слайдовой пары

То, что известны значения Y_L' и Y_R , дает нам информацию о значении входа функции $F20'$. Так как значения Y_R' Y_L тоже известны, то легко можно определить значение выхода этой же F-функции, которое будет равно 0100. Так как перед выходом из F-функции данные подвергаются перестановке, то, сделав шаг назад, находим, что на выходе S-блоков появляется значение 0001. То есть 00 будет являться выходом $S0$ блока, а 01 – выходом $S1$ блока.

Входное сообщение F-функции подвергается перестановке с расширением, а значит вход F-функции 1010 преобразуется к значению 01010101, которое и будет сложено с ключом $K = (K1, K2)$. То есть получается, что вход $S0$ блока $0101 \oplus K1$ даст на выходе значение 00, а вход $S1$ блока $0101 \oplus K2$ – значение 01.

Воспользовавшись табл. 3, можно определить, что значение 00 появляется на выходе $S0$ блока в случае, если на его вход поступило одно из следующих значений: 0010, 0111 или 1000. Таким образом, добавив к каждому из возмож-

ных значений входа значение 0101, получим возможные значения K1. Это будут значения 0111, 0010 или 1000.

Аналогичным образом определяем, что значение 01 появляется на выходе S1 блока в случае, если на его вход поступило одно из следующих значений: 0000, 0010, 0101, 1011 или 1100. А значит, добавив к каждому из возможных значений входа значение 0101, получим возможные значения K2. Это будут значения 0101, 0111, 0000, 1110 или 1001.

Так как во всех раундах шифрования использовался один и тот же ключ, то для первого и последнего раундов должны совпадать значения K1 и K2. Сопоставив, все возможные значения K1 и K2, можно увидеть, что есть только одно значение K1 = 0010, использование которого возможно как в первом, так в последнем раундах, и только одно значение K2 = 0101, использование которого также возможно как в первом, так и в последнем раундах. Таким образом, найден искомый ключ K = 00100101. Убедиться в его правильности можно, зашифровав на нем сгенерированные нами открытые тексты, и сравнив результаты шифрования. Подробнее об этом можно найти информацию в работе [4].

Список литературы:

1. Biryukov A. & Wagner D. Slide Attacks. *Proceedings of Fast Software Encryption'99*. Vol. 1636. *Lecture Notes in Computer Science*. Pp. 245-259. New York: Springer-Verlag.
2. Biryukov A. & Wagner D. Advanced Slide Attacks. In Preneel B. (Ed.), *Advances in Cryptology. Eurocrypt 2000*. Vol. 1807. *Lecture Notes in Computer Science*. Pp. 589-606. New York: Springer.
3. Столлингс В., Криптография и защита сетей: принципы и практика. М.: Вильямс, 2001.
4. Бабенко Л.К., Ищукова Е.А. *Современные алгоритмы блочного шифрования и методы их анализа*. Москва: Гелиос АРВ, 2006. 376 с.

© 2015, Бабенко Л.К., Ищукова Е.А.
Применение слайдовой атаки для анализа
симметричных блочных шифров

© 2015, Babenko L.K., Ischukova E.A.
The use of a slide attack to analyze of symmetric
block cipher