УДК 004.021

ИССЛЕДОВАНИЕ АЛГОРИТМОВ АНАЛИЗА ШИФРА CLEFIA

Ищукова Е.А., Куликов А.В.

Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, Таганрог, e-mail: uaishukova@sfedu.ru;

В статье рассмотрен симметричный блочный алгоритм шифрования CLEFIA, представляющий собой обобщенную структуру Фейстеля. Данный алгоритм шифрования в 2012 г. был включен в международный стандарт облегченного шифрования ISO/IEC. В статье представлены результаты анализа основных криптографических операций, используемых в CLEFIA. Также был проанализирован Механизм переключения рассеивания (Diffusion Switching Mechanism – DSM), чередующий блоки замены и матрицы рассеивания. С целью оценки вклада механизма DSM в повышение криптографической стойкости к дифференциальному криптоанализу были проанализированы различные вариации упрощений алгоритма шифрования CLEFIA. В качестве упрощений были рассмотрены как уменьшение количества раундов шифрования, так и ослабление механизма DSM в виде отключения чередования блоков замены и/или матриц рассеивания. В результате работы был проанализирован DSM механизм, его степень влияния на стойкость шифра к дифференциальному классу атак. Перебор грубой силой для упрощённого шифра из девяти раундов можно осуществить со сложностью $1/2^{128}$, в то время как дифференциальным анализом удалось достигнуть результата в $1/2^{12539}$. В работе представлены экспериментальные результата анализа. Было показано, что использование DSM-механизма в составе алгоритма шифрования CLEFIA не случайно, а имеет обоснованные причины использования.

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

RESEARCH OF CLEFIA CIPHER ANALYSIS ALGORITHMS

Ishchukova E.A., Kulikov A.V.

Southern Federal University, Institute of Computer and Information Security, Taganrog, e-mail: uaishukova@sfedu.ru

The article considers the CLEFIA block encryption algorithm, which is a generalized Feistel structure. In 2012, this encryption algorithm was included in the ISO / IEC international lightweight encryption standard. The article presents the results of the analysis of cryptographic primitives used in CLEFIA. A Diffusion Switching Mechanism (DSM) was also analyzed, alternating between replacement blocks and dispersion matrices. In order to assess the contribution of the DSM mechanism to increasing the cryptographic resistance to differential cryptanalysis, various variations of the CLEFIA encryption algorithm simplifications were analyzed. So among the simplifications was both a reduction in the number of encryption rounds and a weakening of the DSM mechanism in the form of disabling the alternation of replacement blocks and/or dispersion matrices. As a result of the work, the DSM mechanism was analyzed, its degree of influence on the resistance of the cipher to the differential class of attacks. Brute force brute force for a simplified cipher of 9 rounds can be performed with complexity $1/2^{128}$, while differential analysis managed to achieve a result of $1/2^{125.39}$. The paper presents experimental analysis results. It was shown that the use of the DSM mechanism as part of the CLEFIA encryption algorithm is not accidental, but has reasonable reasons for using it.

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

CLEFIA – блочный алгоритм шифрования, в основе конструкции которого лежит структура Фейстеля. На вход данный алгоритм шифрования ожидает 128 бит, которые в дальнейшем разбиваются на 4 части по 32 бита. Алгоритм шифрования авторами позиционируется как легковесный, и в 2012 г. организации ISO и IEC включили алгоритм CLEFIA в международный стандарт облегчённого шифрования ISO/IEC 29192-2:2012 [1]. Одной из ключевых особенностей в проектировании данного алгоритма шифрования является использование так называемого Механизма переключения рассеивания (Diffusion Switching Mechanism – DSM), благодаря которому обеспечивается использование различный F-функций в разных раундах шифрования [2]. Механизм подразумевает чередование криптографических примитивов в виде блоков замены и матриц рассеивания. Согласно данному механизму, различается принцип использования математических F-функций. Для четных и нечетных F-функций различается порядок использования блоков замен S0 и S1, а также используются различные матрицы M0 и M1 для перемножения данных.

Цель работы: исследовать влияние механизма DSM на стойкость алгоритма CLEFIA.

Материалы и методы: алгоритм шифрования CLEFIA, метод дифференциального криптоанализа, ПЭВМ AMD Ryzen 5 1600 Six-Core Processor, язык программирования Python.

Алгоритм CLEFIA подразумевает использование четырех веток. Преобразование открытого текста может выполняться под воздействием секретного ключа длиной 128, 192 или 256 бит. В зависимости от этого преобразование будет выполнять-

ся в течение 18, 22 и 26 раундов соответственно. В данной статье анализировался шифр с четырьмя ветками и ключом, размером 128 бит. Через $GFN_{d,r}$ мы обозначим d-веточную и r-раундовую функцию используемую в CLEFIA.

Буквой T обозначим промежуточное значение, RK_i – раундовый ключ, необходимый для вычислений, а X и Y тексты на входе и выходе соответственно. Тогда алгоритм $GFN_{d,r}$ можно расписать следующим образом:

Шаг 1. $T_0 \mid T_1 \mid T_2 \mid T_3 \leftarrow X_0 \mid X_1 \mid X_2 \mid X_3$.

Шаг 2. От i = 0 до r $-$ 1 делать следующее:

Шаг 2.1 $T_1 \leftarrow T_1 \oplus F_0(RK_{2i}, T_0), \quad T_3 \leftarrow T_3 \oplus F_1(RK_{2i+1}, T_2)$.

Шаг 2.2 $T_0 \mid T_1 \mid T_2 \mid T_3 \leftarrow T_1 \mid T_2 \mid T_3 \mid T_0$.

Шаг 3. $Y_0 \mid Y_1 \mid Y_2 \mid Y_3 \leftarrow T_3 \mid T_0 \mid T_1 \mid T_2$.

$$GFN_{8,r}: \begin{cases} \{\{0,1\}^{32}\}^{4r} \times \{\{0,1\}^{32}\}^8 \to \{\{0,1\}^{32}\}^8 \\ (RK_{0(32)}, \ldots, RK_{4r-1(32)}, X_{0(32)}, \ldots, X_{7(32)}) \mapsto Y_{0(32)}, \ldots, Y_{7(32)} \end{cases}.$$

Шаг 1. $T_0 \mid T_1 \mid \ldots \mid T_3 \leftarrow X_0 \mid X_1 \mid \ldots \mid X_7$.

Шаг 2. От i = 0 до r $-$ 1 делать следующее:

Шаг 2.1 $T_1 \leftarrow T_1 \oplus F_0(RK_{4i}, T_0), \quad T_3 \leftarrow T_3 \oplus F_1(RK_{4i+1}, T_2),$

$T_5 \leftarrow T_5 \oplus F_0(RK_{4i+2}, T_4), \quad T_7 \leftarrow T_7 \oplus F_1(RK_{4i+3}, T_6)$.

Шаг 2.2 $T_0 \mid T_1 \mid \ldots \mid T_6 \mid T_7 \leftarrow T_1 \mid T_2 \mid \ldots \mid T_7 \mid T_0$.

Шаг 3. $Y_0 \mid Y_1 \mid \ldots \mid Y_6 \mid Y_7 \leftarrow T_7 \mid T_0 \mid \ldots \mid T_5 \mid T_6$.

Обратная функция $GFN_{d,r}^{-1}$ использует подключи RK_i в обратном порядке, также меняется направление сдвигов на этапах 2.2 и 3.

Алгоритм обработки данных CLEFIA можно представить функцией ENC_r для зашифровки и DEC_r для расшифровки. Эти функции используют структуру $GFN_{4,r}$, которая фактически представляет собой сеть Фейстеля с четырьмя ветками. Обозначим пару значений открытый текст – шифрованный текст как $P, C \in \{0,1\}^{128}$. Будем считать, что каждый текст может содержать 4 фрагмента $P_i, C_i \in \{0,1\}^{32}$ $(0 \le i < 4)$, где $P = P_0 \mid P_1 \mid P_2 \mid P_3$ и $C = C_0 \mid C_1 \mid C_2 \mid C_3$. Обозначим как $WK_0, WK_1, WK_2, WK_3 \in \{0,1\}^{32}$ отбеливающие подключи и обозначим как $RK_i \in \{0,1\}^{32}$ $(0 \le i < 2r)$ раундовые подключи. Функция DEC_r является обратной по отношению к функции ENC_r, за счёт использования обратной функции $GFN_{d,r}^{-1}$. На рис. 1 проилюстрирована функция ENC_r.

Алгоритм выработки раундовых подключей подразумевает различную реализацию для 128, 192 и 256 бит ключа. Так как в данной статье рассматривается версия алгоритм шифрования для секретного ключа размерностью 128 бит, то в дальнейшем будет рассмотрен алгоритм выработки раундовых подключей для 128-битного секретного ключа.

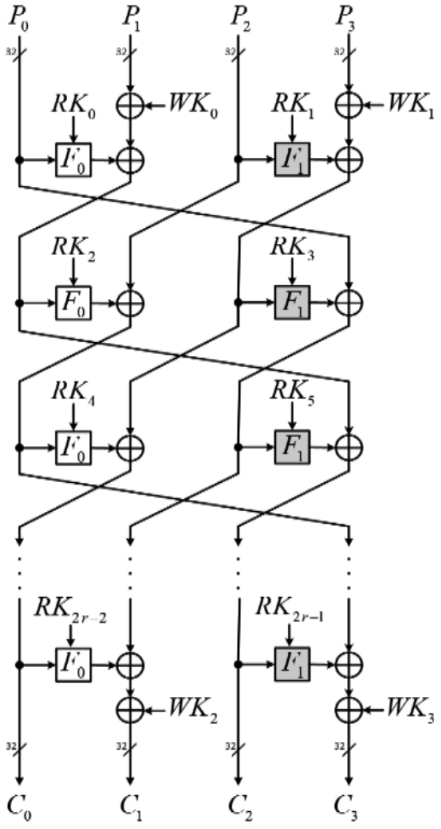

Рис. 1. Функция ENCr

Определим функцию *DoubleSwap*, используемую при выработке ключей, следующим образом:

$$X_{(128)} \mapsto Y_{(128)}$$
$$Y = X[7-63] \,|\, X[121-127] \,|\, X[0-6] \,|\, X[64-120],$$

где $X[a-b]$ обозначает битовую строку, вырезанную начиная с бита *a* по бит *b* из строки *X*.

Алгоритм выработки раундовых подключей делится на две логические части: генерация промежуточного ключа *L* из исходного секретного ключа *K* и расширение *K* и *L* с целью генерации WK_i и RK_i. Промежуточный ключ *L* имеет длину 128 бит. Он генерируется с помощью функции $GFN_{4,12}$, на вход которой в качестве данных поступает значение секретного ключа $K = K_0 \,|\, K_1 \,|\, K_2 \,|\, K_3$. При этом для преобразования в качестве раундовых подключей используется двадцать четыре 32-битных константы $CON_i^{(128)}$ $(0 \le i < 24)$. Таким образом раундовые ключи *K* и промежуточный ключ *L* используются для генерации отбеливающих подключей WK_i $(0 \le i < 4)$ и раундовых подключей RK_j $(0 \le j < 36)$. На следующем шаге используется тридцать шесть 32-битных константных значений $CON_i^{(128)}$ $(24 \le i < 60)$. Таким образом получается, что для генерации всех подключей требуется шестьдесят константных значений.

(Генерация L из K)

Шаг 1. $L \leftarrow GFN_{4,12}(CON_0^{(128)},\ldots,CON_{23}^{(128)},K_0,\ldots,K_3)$.

(*Расширение K и L*)

Шаг 2. $WK_0 \,|\, WK_1 \,|\, WK_2 \,|\, WK_3 \leftarrow K$.

Шаг 3. От i = 0 до 8 делать следующее:

$T \leftarrow L \oplus (CON_{24+4i}^{(128)} \,|\, CON_{24+4i+1}^{(128)} \,|\, CON_{24+4i+2}^{(128)} \,|\, CON_{24+4i+3}^{(128)})$,

$L \leftarrow \sum(L)$,

если i нечётное, то: $T \leftarrow T \oplus K$,

$RK_{4i} \,|\, RK_{4i+1} \,|\, RK_{4i+2} \,|\, RK_{4i+3} \leftarrow T$.

Функция F, используемая в процессе шифрования, имеет две реализации: F_1 и F_2. В самих функциях используются матрицы рассеивания, обозначаемые как M, и блоки замены, обозначаемые S. Работу каждой из F-функций можно описать следующим образом:

$[F-$ *функция* $F_0]$	$[F-$*функция* $F_1]$
Шаг 1. $T \leftarrow RK \oplus x$.	Шаг 1. $T \leftarrow RK \oplus x$.
Шаг 2. Пусть $T = T_0 \,|\, T_1 \,|\, T_2 \,|\, T_3$, $T_i \in \{0,1\}^8$.	Шаг 2. *Пусть* $T = T_0 \,|\, T_1 \,|\, T_2 \,|\, T_3, T_i \in \{0,1\}^8$.
$T_0 = S_0(T_0)$, $T_1 = S_1(T_1)$.	$T_0 = S_1(T_0)$, $T_1 = S_0(T_1)$.
$T_2 = S_0(T_2)$, $T_3 = S_1(T_3)$.	$T_2 = S_1(T_2)$, $T_3 = S_0(T_3)$.
Шаг 3. Пусть $y = y_0 \,|\, y_1 \,|\, y_2 \,|\, y_3$, $y_i \in \{0,1\}^8$.	Шаг 3. Пусть $y = y_0 \,|\, y_1 \,|\, y_2 \,|\, y_3$, $y_i \in \{0,1\}^8$.
$'(y_0, y_1, y_2, y_3) = M_0\,'(T_0, T_1, T_2, T_3)$.	$'(y_0, y_1, y_2, y_3) = M_0\,'(T_0, T_1, T_2, T_3)$.

S_0 и S_1 представляют собой нелинейные 8-битные S-блоки. При этом в каждой из F-функций используется свой порядок применения S-блоков. Также разные F-функции используют на шаге 3 разные матрицы (M_0 и M_1). Матрицы имеют следующий вид (значения в матрице представлены в 16-ричном виде, *a* соответствует значению 10):

$$M_0 = \begin{pmatrix} 0x01 & 0x02 & 0x04 & 0x06 \\ 0x02 & 0x01 & 0x06 & 0x04 \\ 0x04 & 0x06 & 0x01 & 0x02 \\ 0x06 & 0x04 & 0x02 & 0x01 \end{pmatrix}, \quad M_1 = \begin{pmatrix} 0x01 & 0x08 & 0x02 & 0x0a \\ 0x08 & 0x01 & 0x0a & 0x02 \\ 0x02 & 0x0a & 0x01 & 0x08 \\ 0x0a & 0x02 & 0x08 & 0x01 \end{pmatrix}.$$

При этом полиномиальное перемножение между матрицами и векторами производится в поле $GF(2^8)$. В качестве нормализующего полинома используется полиномом $z^8 + z^4 + z^3 + z^2 + 1$. Структура для функций F_0 и F_1 приведена на рис. 2.

Чередование матриц рассеивания и блоков замены, а также различные алгебраические структуры, лежащие в основе блоков замены, представляют собой Механизм переключения рассеивания. Изучение влияния данного Механизма переключения рассеивания на стойкость исследуемого алгоритма шифрования является одной из целей настоящего исследования.

В качестве метода исследования нами был выбран метод дифференциального криптоанализа, как один из наиболее популярных методов анализа симметричных блочных шифров [2]. Метод дифференциального криптоанализа рассматривает пары текстов при их изменении в зависимости от действий, совершаемых в каждом раунде. Впервые метод дифференциального криптоанализа был применен Э. Бихамом и А. Шамиром к анализу алгоритма шифрования DES [3, 4]. Сейчас этот метод широко применяется к анализу большинства шифров. В качестве дифференциала или разности рассматривается результат операции поразрядного сложения данных по модулю 2.

Матрицы рассеивания M_0 и M_1 размером 4x4 делят текст, поданный на вход, на 4 части по 8 бит, а далее эти 4 части подставляются в следующие уравнения:

$$(x_1, x_2, x_3, x_4) = X.$$

$$x_1' = \{01\}x_1 + \{02\}x_2 + \{04\}x_3 + \{06\}x_4.$$

$$x_2' = \{02\}x_1 + \{01\}x_2 + \{06\}x_3 + \{04\}x_4.$$

$$x_3' = \{04\}x_1 + \{06\}x_2 + \{01\}x_3 + \{02\}x_4.$$

$$x_4' = \{06\}x_1 + \{04\}x_2 + \{02\}x_3 + \{01\}x_4.$$

$$X' = (x_1', x_2', x_3', x_4').$$

Все вычисления необходимо выполнять в поле $GF(2^8)$ над многочленом $z^8 + z^4 + z^3 + z^2 + 1$, что подразумевает трактовку сложения как операцию побитового xor, а умножения – как перемножения двух полиномов по модулю $z^8 + z^4 + z^3 + z^2 + 1$ [5, 6]. Коэффициенты перед x представляют собой полиномы, которые выглядят следующим образом: $\{01\} = x^0; \{02\} = x^1; \{04\} = x^2; \{06\} = x^2 + x^1$.

В первую очередь в ходе анализа была доказана обратимость матриц рассеивания по отношению к самим себе. Это позволяет нам легче находить удобную характеристику, если необходимо получить некоторую разность, которая дважды будет проходить через одну матрицу рассеивания. Следующим этапом было проанализировано поведение различных входов.

$$\begin{bmatrix} \Delta x \\ 0 \\ 0 \\ 0 \end{bmatrix} \boxed{M_0} \begin{bmatrix} \Delta x \\ 2\bullet\Delta x \\ 4\bullet\Delta x \\ 6\bullet\Delta x \end{bmatrix} \begin{bmatrix} \Delta x \\ 2\bullet\Delta x \\ 0 \\ 0 \end{bmatrix} \boxed{M_0} \begin{bmatrix} 5\bullet\Delta x \\ 0 \\ 8\bullet\Delta x \\ E\bullet\Delta x \end{bmatrix}$$

Учитывая обратимость матрицы самой себе, можно получить следующую закономерность: при 1 ненулевом входе, мы всегда будем получать 4 ненулевых выхода, подавая 2 ненулевых выхода, мы получим 3–4 ненулевых, при подаче 3 ненулевых мы можем получить на выходе от 2 до 4 ненулевых текстов и, подавая 4 ненулевых текста, на выходе получаем от 1 до 4 ненулевых текстов. Количество ненулевых выходов зависит от того, какие коэффициенты будут подобраны [5].

В ходе анализа блоков замены было выяснено, что блоки замены S_0 представляют больший интерес в рамках дифференциального криптоанализа, так как вероятность преобразования одной разности в другую у данного блока замены может достичь более высоких вероятностей по сравнению с S_1 [6].

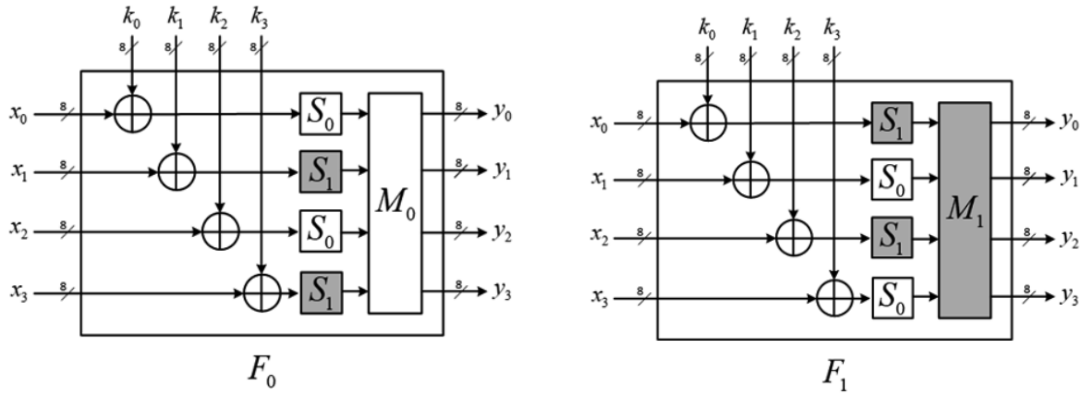

Рис. 2. Функции F_0 и F_1

Данный вывод легко сделать, обратив внимание на табл. 1.

Для анализа DSM механизма было необходимо ограничить область воздействия данного механизма или полностью его отключить. Отключение и ограничение подразумевают собой исключение разнообразия блоков замены и/или матриц рассеивания. Таким образом, к примеру, будут использоваться только S_0, даже там, где должен был быть блок замены S_1. То же касается матриц рассеивания.

Результаты исследования и их обсуждение

В ходе работы были проанализированы следующие вариации упрощений: шесть раундов без разнообразия M и S блоков, двенадцать раундов без разнообразия M и S блоков, двенадцать раундов без разнообразия M блоков, шесть раундов с DSM механизмом и девять раундов с DSM механизмом. Вариации с шестью раундами использовались не столько для получения сложности нахождения дифференциальной характеристики, сколько для того, чтобы убедиться в правильности найденных характеристик с помощью персонального компьютера. Таким образом шестираундовые характеристики были вручную найдены на персональном компьютере, в то время как остальные были разработаны теоретически. Перебор и вычисления осуществлялись с помощью ПЭВМ со следующими характеристиками: процессор AMD Ryzen 5 1600 Six-Core Processor.

Для проведения полного анализа механизма DSM были проведены эксперименты для различных вариантов использования блоков замены и матриц M_0 и M_1. были по очереди отключены разнообразия блоков замены и матриц M. В ходе работы были разработаны алгоритмы анализа с учетом различных вариантов упрощений шифра. Кроме того, чтобы иметь возможность оценить влияние DSM-механизма в полной мере, были построены дифференциальные характеристики для различного числа раундов шифрования (от 6 до 12) и для них теоретически просчитаны значения вероятностей. Результаты теоретических расчетов и практических экспериментальных данных сведены в табл. 2. В каждом эксперименте было атаковано 8 бит ключа.

Можно видеть, что при использовании только одной матрицы M_0 в DSM-механизме, сложность анализа 12 раундов будет ниже сложности анализа 9 раундов, где используются обе матрицы M_0 и M_1. Это связано с тем, что в случае с двумя матрицами M_0 и M_1, чем больше раундов, тем тяжелее подобрать удобные разности для построения итогового дифференциала. В ходе анализа было показано, что при использовании обеих матриц M_0 и M_1 невозможно получить одинаковые выходы разностей при использовании одинаковых разностей на входах в F-функцию. Одним из приемов, который часто используется в дифференциальном криптоанализе, является пропуск некоторых преобразований, где на вход поступает разность, равная нулю. В данном же случае, при использовании разных матриц M_0 и M_1, выявленное свойство не позволяет пропускать преобразования и вероятность начинает уменьшаться слишком быстро.

Таблица 1

Таблица со статистикой преобразований в блоках замены

Вероятность	n	S_0	S_1	Вероятность	n	S_0	S_1
0	0	40022	33151	$\approx 1/2^{5,41}$	6	848	0
$1/2^7$	2	19501	32130	$1/2^5$	8	119	0
$1/2^6$	4	5037	255	$\approx 1/2^{4,68}$	10	9	0

Таблица 2

Сложность анализа в зависимости от конфигурации алгоритма

Раунды	S	M	Реализация	Итоговая сложность
6	только S_0	только M_0	практическая	$1/2^{14,04}$
6	S_0 и S_1	M_0 и M_1	практическая	$1/2^{16,36}$
9	S_0 и S_1	M_0 и M_1	теоретическая	$1/2^{125,39}$
12	только S_0	только M_0	теоретическая	$1/2^{94,7}$
12	S_0 и S_1	только M_0	теоретическая	$1/2^{95}$

При использовании в каждой F-функции одинаковых матриц в результате анализа удалось построить характеристику для 12 раундов шифрования. Вероятность появления такой характеристики составила $1/2^{94,7}$. В то же время при использовании разных матриц M_0 и M_1 удалось построить характеристику только для 9 раундов. При этом вероятность появления такой характеристики оказалась слишком маленькой $1/2^{125,39}$, что слишком близко к полному перебору.

Аналогичный эксперимент проводился и для чередования S-блоков замены. Было показано, что для блока S_0 в таблице присутствуют более высокие значения вероятностей, чем для блока S_1. Также было показано, что для блоков S_0 и S_1 одинаковые значения входных разностей очень часто не могут быть преобразованы к одинаковым значениям разностей на выходе, что сильно затрудняет построение многораундовых характеристик.

Заключение

В результате проделанной работы было показано, что использование DSM-механизма в составе алгоритма шифрования CLEFIA не случайно, а имеет обоснованные причины использования. Наличие DSM-механизма значительно увеличивает сложность анализа шифра. Как следствие, при рассмотрении варианта шифра с использованием DSM-механизма можно проанализировать гораздо меньше раундов шифрования, чем при рассмотрении шифра без DSM-механизма.

Работа выполнена при поддержке гранта РФФИ № 17-07-00654 «Разработка и исследование последовательных и параллельных алгоритмов анализа современных симметричных шифров с использованием технологий MPI, NVIDIA CUDA, SageMath».

Список литературы

1. ISO. ISO/IEC 29192-2:2012. [Электронный ресурс]. URL: https://www.iso.org/standard/56552.html (date of access: 08.11.2019).

2. Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, Tetsu Iwata The 128-bit Blockcipher CLEFIA (Extended Abstract) [Электронный ресурс]. URL: https://www.iacr.org/archive/fse2007/45930182/45930182.pdf (date of access: 08.11.2019).

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

4. Biham E., Shamir A. Differential Cryptanalysis of DES-like Cryptosystems, Extended Abstract. Crypto'90. SpringerVelgar, 1998. 105 p.

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

6. Ищукова Е.А., Калмыков И.А. Дифференциальные свойства S-блоков замены для алгоритма ГОСТ 28147-89 // Инженерный вестник Дона. 2015. № 4 [Электронный ресурс]. URL: ivdon.ru/ru/ magazine/archive/n4y2015/3284 (дата обращения: 08.11.2019).