УДК 681.03.245 DOI 10.18522/2311-3103-2016-9-2736

Л.К. Бабенко, Е.А. Ищукова, Д.М. Алексеев, А.В. Красовский, М.В. Письменский

КОМПЛЕКСНЫЙ ПОДХОД К ОЦЕНКЕ НАДЕЖНОСТИ СТАНДАРТА ГОСТ Р 34.12-2015*

Целью представленной работы является разработка, реализация и исследование последовательных и параллельных алгоритмов оценки надежности двух шифров, входящих в состав нового стандарта симметричного шифрования данных ГОСТ Р 34.12-2015 с использованием различных видов криптоанализа, а именно: линейного анализа, слайдовой атаки и производных методов дифференциального анализа, таких как метод невозможных дифференциалов и метод анализа на связанных ключах. При проведении исследований рассмотрены два алгоритм симметричного шифрования, входящие в состав нового стандарта РФ ГОСТ Р34.12-2015. Данные шифры имеют различную схему построения: алгоритм Магма построен на основе сети Фейстеля, а алгоритм Кузнечик – по принципу SP-сети. Таким образом, исследованы свойства надежности для двух основных схем построения современных алгоритмов симметричного блочного шифрования. Одним из способов повышения производительности при анализе различных криптосистем является использование распределенных многопроцессорных вычислений для ускорения процесса анализа и скорейшего получения результата. В работе для этого использована технология MPI. Одним из достоинств программ, разработанных с использованием библиотеки MPI, является возможность их использования как на специально оборудованном кластере, так и на кластере, состоящем из обычных ПЭВМ, связанных между собой сетью. В результате работы были разработаны, реализованы и опробованы последовательные и параллельные алгоритмы анализа стойкости шифров, входящих в состав проекта нового стандарта шифрования данных в нашей стране. Программы выполнены в среде MS Visual Studio C++. Для параллельных программ использован пакет MPICH для выполнения многопроцессорных вычислений. В результате исследования разработанных и реализованных алгоритмов получены обширные экспериментальные данные, систематизированные в виде таблиц и графиков. Полученные алгоритмы и реализации в дальнейшем можно будет использовать для анализа других блочных шифров, обладающих схожей структурой.

Криптография; блочный шифр; схема Фейстеля; SP-сеть; дифференциальный анализ; линейный анализ; слайдовая атака; невозможные дифференциалы; связанные ключи; секретный ключ.

L.K. Babenko, E.A. Ishchukova, D.M. Alekseev, A.V. Krasovsky, M.V. Pismensky

INTEGRATED APPROACH TO THE ASSESSMENT OF RELIABILITY OF GOST R34.12-2015 STANDARD

The aim of this work is the development, implementation and investigation of sequential and parallel algorithms for evaluating the reliability of two ciphers that are a part of the new symmetric cipher's standard GOST R 34.12-2015. The analysis is carried out using different types of cryptanalysis, namely: linear analysis, slide attacks and derivative methods for differential analysis, such as the method of impossible differentials and the method of related-key attack. Examined are two symmetric encryption algorithms that make up the new Russian standard GOST R34.12-2015. These ciphers have a different construction of the scheme: Magma algorithm is based on a Feistel network, and Kuznyechik algorithm is on the basis of SP-network. Thus, reliability properties are investigated for construction of two basic schemes for modern symmetric block encryption algorithm. One way to improve performance in the analysis of various cryptosystems is to use a distributed multiprocessor computing to accelerate the process of analysis and get the result as soon as possible. The MPI technology is used in the paper. One of the advantages of programs developed using the

* Работа выполнена при поддержке гранта РФФИ № 15-37-20007_мол_а_вед.

MPI library is the possibility of their use as a specially equipped cluster, and the cluster of conventional PC linked by a network. As a result, sequential and parallel algorithms were designed, implemented, and tested for resistance investigation of ciphers included in the project of a new data encryption standard in our country. Programs were implemented in the environment of MS Visual Studio C ++. For parallel programming used was the MPICH package to perform multiprocessor computing. The study of developed and implemented algorithms resulted in extensive experimental data, systematized in the form of tables and graphs. These algorithms and implementation in the future could be used for analysis of other block ciphers that have a similar structure.

Cryptography; block cipher; Feistel scheme; SP-network; differential analysis; linear analysis; slide attack; impossible differential analysis; related keys; secret key.

Введение. Летом 2015 года был представлен проект нового стандарта шифрования данных, а в январе 2016 он был принят как ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» [1]. Стандарт включает в себя описание двух блочных шифров. Первый – с размером блока 64 бит – основан на старом ГОСТ 28147-89 с зафиксированными блоками замены и имеет название «Магма». Второй – с размером блока 128 бит – новый шифр типа «подстановочно-перестановочная сеть» описан под именем «Кузнечик».

Постановка задачи. Настоящая работа посвящена изучению принятого стандарта шифрования ГОСТ Р 34.12-2015 с использованием различных методов анализа, что является актуальной задачей в связи с его недавним принятием.

1. Алгоритм шифрования Магма. Алгоритм шифрования Магма является наследником стандарта ГОСТ 28147-89 с тем отличием, что для шифра Магма были зафиксированы блоки замены. 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-ой раунд ключи инвертируются и имеют вид K8 – K1. После выполнения 32-х раундов шифрования левая и правая часть «склеиваются», образуя результат работы алгоритма – блок шифр-текста. Расшифрование выполняется аналогично, изменяется лишь порядок ключей – он инвертируется относительно зашифрования. (термины: Расшифрование – дешифрование; зашифрование – шифрование) Согласна с тем, что эти слова – синонимы. Однако ранее мне неоднократно делали замечание, где говорилось, что правильно использовать именно связку зашифрование-расшифрование.

Более подробное описание шифра можно найти в работах [1,2].

2. Алгоритм шифрования Кузнечик. Шифр Кузнечик представляет собой симметричный алгоритм блочного шифрования с размером блока 128 бит и длиной ключа 256 бит, для генерации которого используется сеть Фейстеля.

При реализации алгоритма шифрования используется три базовых преобразования: сложение данных с раундовым ключом по модулю 2 (операция X), табличная замена байтов (операция S), линейное перемешивание байтов (операция L). Более подробно описание данных операций можно найти в работах [1, 3].

Алгоритм развертывания ключа использует итерационные константы $C_i \in V_{128}$, i = 1, 2, …, 32, которые определены следующим образом:

$$C_i = L(Vec_{128}(i)), i = 1, 2, \ldots, 32.$$

Итерационные ключи $K_i \in V_{128}$, i = 1, 2, …, 10, вырабатываются на основе ключа:

$$K = k_{255}||\ldots||k_0 \in V_{256},\ k_i \in V_1,\ i = 0, 1, \ldots, 255,$$

и определяются равенствами:

$$K_1 = k_{255}||\ldots||k_{128};$$

$$K_2 = k_{127}||\ldots||k_0;$$

$$(K_{2i+1}, K_{2i+2}) = F\,[C_{8(i-1)+8}]\ldots F\,[C_{8(i-1)+1}](K_{2i-1}, K_{2i}),\ i = 1, 2, 3, 4.$$

Алгоритм шифрования в зависимости от значений итерационных ключей $K_i \in V_{128}$, $i = 1, 2, \ldots, 10$, реализует подстановку $E_{K1, \ldots, K10}$, заданную на множестве V_{128} в соответствии с равенством:

$$E_{K1, \ldots, K10}(a) = X[K_{10}]LSX[K_9]\ldots LSX[K_2]LSX[K_1](a),$$

где $a \in V_{128}$.

Размер блока для шифра «Кузнечик» составляет 128 бит. После того, как соответствующий блок подан на вход для шифрования, его необходимо сложить по модулю два с первым раундовым подключом K_1, затем выполнить девять раундов преобразований. Раунд включает три операции: табличная замена с помощью блока S, перемешивание информации с помощью преобразования L и сложение по модулю два с раундовым подключом K_{1+i}, где i – номер соответствующего раунда. После 9 раундов преобразований блок открытого текста становится 128-битным блоком шифр-текста.

3. Обзор применяемых методов анализа. Метод ***слайдовой атаки*** впервые был предложен А. Бирюковым и Д. Вагнером [4, 5]. 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.

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 шифрования системой линейных аналогов [6, 7]. Существенным недостатком метода является необходимость в больших объемах данных, зашифрованных на одном и том же секретном ключе, что осложняет практическое применение к анализу шифра.

Для успешного применения метода линейного криптоанализа необходимо решить следующие задачи. Найти наиболее эффективные статистические линейные аналоги. При нахождении аналогов обратить внимание на то, что в них должно быть задействовано как можно больше битов искомого секретного ключа К. Получить статистические данные: необходимый объем пар текстов (открытый – закрытый текст), зашифрованных с помощью анализируемого алгоритма на одном и том же секретном ключе. Определить ключ (или некоторые биты ключа) путем анализа статистических данных с помощью линейных аналогов [7].

Метод ***невозможных дифференциалов*** – метод криптоанализа блочных шифров предложенный Э. Бихамом, А. Шамиром и А. Бирюковым в 1998 году. Его применяли ко многим усеченным версиям шифров, таких как IDEA,AES,Khufu и Khafre, Skipjack, MISTY и KASUMI, S-AES [8–11].

Суть метода невозможных дифференциалов 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.

Атаки со связанными ключами относятся к дифференциальному типу и были впервые предложены Э. Бихамом в соавторстве с Ор. Данкеламном и Н. Келлером [12–13]. Основной идеей метода является наличие нескольких взаимосвязанных ключей шифрования, связь которых определяется в соответствии с некоторой функцией F. Данная функция известна аналитику и выбирается им же.

Самым известным применением взаимосвязанных ключей стали атаки на AES-256 и AES-192, представленные А. Бирюковым и Д. Ховратовичем [14], где они смогли сократить сложность нахождения ключа и доказать теоретическую уязвимость шифра. Так же существуют работы с применением данного типа атаки на шифр ГОСТ [15, 16].

4. Линейные и дифференциальные свойства ГОСТ Р 34.12-2015. Авторами настоящей работы ранее был выполнен предварительный анализ криптографических примитивов, входящих в состав шифров стандарта ГОСТ Р34.12-2015. Анализ S-блоков замены для определения дифференциальных свойств алгоритма Магма, приведен в работе [17], линейных свойств – в работе [18].

Чтобы определить дифференциальные свойства алгоритма Кузнечик, достаточно определить дифференциальные свойства элементов, его составляющих. Так как данный шифр состоит из преобразований S, L, X, то именно эти операции и были рассмотрены.

Было показано, что дифференциальное свойство X преобразования заключается в том, что выходной дифференциал представляет из себя результат операции сложения по модулю 2 входного дифференциала и дополнительного, т.е. выходной и входной дифференциал равны при одинаковых дополнениях и не равны при разных дополнениях.

Дифференциальное свойство L преобразования заключается в том, что выходной дифференциал представляет из себя результат преобразования L над входным дифференциалом.

Дифференциальное свойство S преобразования заключается в том, что существует неравномерность распределения выходных дифференциалов. Для S-блока была построена таблица анализа в соответствии с алгоритмом, приведенным в работе [17].

5. Разработка и реализация алгоритмов анализа шифра Магма с использованием метода невозможных дифференциалов. В рамках данной работе рассматривается упрощенный алгоритм Магма, в котором операция сложения по модулю 2^{32} заменена на побитовое сложение по модулю 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.

Для побитового сложения по модулю 2 с ключом разность не меняется, этот факт часто используется в дифференциальном криптоанализе. Для замены с помощью S-блоков разность внутри блоков меняется, но наличие разности остается неизменным. 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.

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

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. Имея две эти последовательности, 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 четвертым 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.

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. В результате эксперимента было показано, что метод работает и позволяет отбрасывать неверные значения для части подключа, приходящегося 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. 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}.

6. Анализ алгоритма Кузнечик с использованием связанных ключей. Ранее, в работе [18] авторами была представлена схема для проведения анализа шифра Кузнечик с использованием связанных ключей. В настоящей работе авторы предлагают рассмотреть предложенный ими алгоритм. Обозначим слово в n битов как W_n. Обозначим значение $\Delta K_i^{n,d}$ как дифференциал i-ых подключей ключей n и d. Обозначим K_i^n как i-ый подключ ключа n. Обозначим объединение слов символом $\|$, т.е. $01 \| 11 = 0111$. Обозначим массив конструкций слов как |Элемент|, где "Элемент" обозначает элементарную конструкцию и обозначим её перебор как $|\overset{\cdots}{\text{Элемент}}|$ (вложенность переборов обозначает вложенность циклов переборов).

Алгоритм 1

Данный алгоритм используется для восстановления возможных первых подключей искомого ключа. Далее будет использоваться дифференциал между первым и вторым ключом.

1) Берём произвольное значение закрытого текста $C \in W_{128}$.

2) Расшифровываем данный текст на ключах 1 и 2 и получаем $P_1 \in W_{128}$ и $P_2 \in W_{128}$ соответственно.

3) Вычисляем дифференциал ΔP полученных открытых текстов P_1 и P_2.

4) Вычисляем новое значение $\Delta I = \Delta P \oplus \Delta K_1^{1,2}$, $I \in W_{128}$ и обозначаем его как входной дифференциал.

5) Дифференциал вторых подключей преобразуем с помощью обратной L функции и обозначаем его как выходной дифференциал $\Delta O = L^{-1}(\Delta K_2^{1,2})$, $O \in W_{128}$.

6) Разбиваем входной и выходной дифференциал в соответствии с π преобразованиями на подвходные и подвыходные дифференциалы т.е. $\Delta I = i_0 \parallel i_1 \parallel \cdots \parallel i_{15}$, $i_n \in W_8$, $n = \overline{0,15}$ и $\Delta O = o_0 \parallel o_1 \parallel \cdots \parallel o_{15}$, $o_n \in W_8$, $n = \overline{0,15}$.

7) Для каждого π_n $n = \overline{0,15}$ преобразования перебираем 256 входных пар $(v, v \oplus i_n)$, $v = \overline{0,255}$ $i_n \in \pi_n$ $n = \overline{0,15}$ со значениями, соответствующими подвходному дифференциалу, и сравниваем выходной дифференциал двух значений после этого π-преобразования с соответствующим ему подвыходным дифференциалом. Если они равны, то пары входных значений π преобразования добавляем в соответствующий ему массив $m_n = |(W_8, W_8)|$ и $m_n \in \pi_n$ $n = \overline{0,15}$.

8) После того, как для каждого π-преобразования составлены массивы возможных пар входов $m_n \in \pi_n$ $n = \overline{0,15}$, оставляем в каждом таком массиве значения, соответствующие только для первого ключа, т.е. $m_n \to f_n = |W_8|_n$ $n \in \overline{0,15}$.

9) Находим все возможные сочетания значений массивов $f_n = |W_8|_n$ $n \in \overline{0,15}$ в соответствии со структурой значения для S преобразования, т.е. находим $E = |W_{128}| = \ddot{f}_0 \parallel \ddot{f}_1 \parallel \cdots \parallel \ddot{f}_{15}$.

10) Вычисляем все возможные первые подключи первого ключа $K1 = |W_{128}| = P_1 \oplus \ddot{E}$.

Алгоритм 2

Данный алгоритм используется для восстановления первого (искомого) ключа. Вначале используется **Алгоритм 1** для восстановления первых подключей первого ключа, а затем находятся все возможные вторые подключи. Далее будет использоваться дифференциал между первым и третьим ключом.

1) Выполняем **Алгоритм 1** и получаем массив первых подключей первого ключа K1.

2) Берём произвольное значение закрытого текста $C \in W_{128}$.

3) Расшифровываем данный текст на ключах 1 и 3 и получаем $P_1 \in W_{128}$ и $P_3 \in W_{128}$ соответственно.

4) Вычисляем все возможные значения пары (P_1, P_2) после первого ключа $M_1 = |(W_{128}, W_{128})| = |(P_1 \oplus V, P_3 \oplus V)|$, $V = \ddot{K1}$.

5) Каждое значение пары всех пар в массиве M_1 подвергаем преобразованию S, а затем L: $M_2 = |(W_{128}, W_{128})| = |(LS(P_1 \oplus V), LS(P_3 \oplus V))|$, $V = \ddot{K1}$.

6) Вычисляем дифференциал каждой пары массива M_2 т.е. $M_3 = |W_{128}| = |(LS(P_1 \oplus V) \oplus LS(P_3 \oplus V)|$, $V = \ddot{K1}$.

7) Вычисляем дифференциалы после разницы с вторыми подключами $\Delta I = \Delta K_2^{1,3} \oplus \ddot{M}_3$ и определяем ΔI как массив входных дифференциалов.

8) Определяем значение выходного дифференциала $\Delta O = L^{-1}(\Delta K_3^{1,3})$.

9) Для каждого входного дифференциала $Ie = \ddot{\Delta} I$ и выходного ΔO выполняем пункты 6,7,8,9 из первой части алгоритма в результате чего на каждый Ie элемент массива ΔI мы имеем массив R возможных значений до разницы с вторым подключём первого ключа т.е. если обозначить пункты 6,7,8,9 как функцию R=F(Ie, ΔO), то мы можем получить массив с парами всех возможных первых и вторых подключей т.е.

$$\text{Результат} = |(W_{128}, W_{128})|$$
$$= \left|\left(V, \left|F\left(LS(P_1 \oplus V) \oplus LS(\overset{\cdots}{P_3} \oplus V), L^{-1}\left(\Delta K_3^{1,3}\right)\right)\right| \oplus LS(P_1 \oplus V)\right)\right|,$$
$$V = \ddot{K}1$$

Массив |Результат| следует перебрать для генерации всех остальных подключей и их проверки. Для этого надо перебрать пары первого и второго подключа, относящиеся к первому ключу, и сгенерировать из них остальные 8 подключей. После этого все новые 10 подключей подставляют в такой же алгоритм шифрования, после чего на искомом и собственном шифруется один известный текст и сравниваются результаты (закрытые тексты). Если они равны, то перебираемая на данном этапе пара первого и второго подключей является искомой.

7. Слайдовый анализ для алгоритмов Магма и Кузнечик. Одним из простых вариантов слайдовой атаки является ситуация, когда можно сопоставить один процесс зашифрования с другим таким образом, что один из процессов будет «отставать» от другого на один раунд.

Авторами настоящей работы были рассмотрены подходы к анализу обоих шифров и получены обширные экспериментальные данные. В связи с ограничением объема настоящей статьи, мы предлагаем обратиться к более ранним публикациям, для ознакомления с полученными результатами. Подходы к анализу алгоритма Магма представлены в работах [3, 7, 19], в том числе с использованием параллельной технологии MPI в работах [20].

Если кратко подводить итог, то можно сказать, что для алгоритма шифрования Магма разработан алгоритм поиска слайдовых пар для одноразундового самоподобия. Данный алгоритм реализован с использованием технологии MPI. Экспериментально показано, что для технологии MPI анализ 2^{16} блоков текстов с использованием 4 ядер Intel Core i5 – 3320M CPU, 2.60 Гб в среднем составляет 188.47 мсек. Показано, что поиск слайдовой пары при использовании двух процессов на 2 ядрах занимает в 1,7 раза больше времени, чем аналогичное вычисление для четырех процессов на 4 ядрах. Показано, что время поиска слайдовой пары для алгоритма Магма при переборе 2^{32} текстов с использованием 14 процессоров занимает в среднем 58 минут, с использованием 18 процессоров – 42 минуты.

8. Линейный анализ алгоритма шифрования Магма. Ранее авторами был проведен анализ блоков замены для шифра Магма. Результаты анализа можно найти в работе [18]. В работе [20] показано, как можно используя линейные свойства S-блоков замены строить статистические аналоги для одного раунда шифрования. Для построения аналогов многораундовых характеристик предлагается использовать подход, описанный в работе [3]. Так, например, для трех раундов шифрования, мы можем построить следующий линейный аналог.

Вначале необходимо построить аналоги для первого и третьего раундов шифрования. Возьмем для этого одно из подходящих значений векторов $(\alpha, \beta) = (1101{,}0001)$ для первого блока замены:

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

$$M_{33} \oplus M_{34} \oplus M_{36} \oplus Y_{25}^3 = K_{65} \oplus K_{66} \oplus K_{68}, \quad (2)$$

для обоих аналогов вероятность того, что Q = 0, равна 0,25.

В последнем линейном аналоге присутствуют биты Y_{25} и Y_{25}^3. Их можно получить, сложив по модулю два левую часть выходного сообщения Y и сообщение B, поступающее на вход функции F второго раунда шифрования. Таким образом:

$$Y_{25} = X_{25} \oplus B_{25}; \quad (3)$$

$$Y_{25}^3 = M_{25} \oplus B_{25}; \quad (4)$$

Путем сложения можем объединить аналоги (1) и (2), прибегая к заменам по формулам (3) и (4:)

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

Выводы. С помощью программ, реализованных на основе разработанных алгоритмов, получены, проанализированы и систематизированы обширные экспериментальные данные, отражающие эффективность разработанных алгоритмов. Экспериментальные данные для параллельных алгоритмов отражают зависимость скорости вычислений от используемого числа процессоров и технических характеристик вычислительной системы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Криптографическая защита информации. Блочные шифры. – URL: https://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf.
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., Ломов И.С.* Математическое моделирование криптографического алгоритма «Кузнечик» // Информационное противодействие угрозам терроризма. – 2015. – С. 166-176.
4. *Бирюков А., Вагнер Д.* Слайдовые атаки // Труды быстрого программного шифрования. Лекции в области компьютерных наук. – 1999. – № 1636. – С. 245-259.
5. *Бирюков А., Вагнер Д.* Расширенная слайдовая атака. Достижения в криптологии // Еврокрипт. Лекции в области компьютерных наук. – 2000. – № 1807. – С. 589-606.
6. *Matsui M.* Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology – EUROCRYPT'93, Springer-Verlag, 1998. –386 p.
7. *Бабенко Л.К., Ищукова Е.А*. Современные алгоритмы блочного шифрования и методы их анализа. – М.: Гелиос АРВ, 2006. – 376 с.
8. *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.
9. *Raphael C.-W. Phan*. Impossible Differential Cryptanalysis of Mini-AES // Cryptologia. – October 2003. – No. XXVII (4). – P. 283-292.
10. *Raphael C.-W. Phan, Mohammad Umar Siddiqi* Generalised Impossible Differentials of Advanced Encryption Standard // Electronics Letters. – July 2001. – No. 37 (14). – P. 896-898.
11. *Письменский М.В., Ищукова Е.А.* Криптоанализ S-AES с помощью метода невозможных дифференциалов // «Студенческий научный форум» - 2016. Актуальные проблемы информационной безопасности. – http://www.scienceforum.ru/2016/pdf/24173.pdf.
12. *Eli Biham, Orr Dunkelman, and Nathan Keller*. New results on boomerang and rectangle attacks // In FSE'02. – Springer, 2002. – Vol. 2365 of LNCS.
13. *Eli Biham, Orr Dunkelman, and Nathan Keller*. Related-key boomerang and rectangle attacks // In EUROCRYPT'05. – Springer, 2005. – Vol. 3494 of LNCS. – P. 507-525.
14. *Biryukov A., Khovratovich D., and Iv. Nikoli´c.* Examples of differential multicollisions for 13 and 14 rounds of AES-256, 2009. – http://eprint. iacr.org/2009/242.pdf.
15. *Rudskoy V.* On zero rractical significance of "key recovery attack on full GOST block cipher with zero time and memory", 2010. – http://eprint.iacr.org/2010.
16. *Пудовкина М.А., Хоруженко Г.И.* Атака на шифрсистему ГОСТ 28147-89 с 12 связанными ключами // Математические вопросы криптографиии. – 2013. – Т. 4. – Вып. 2. – Р. 127-152.
17. *Ищукова Е.А., Калмыков И.А.* Дифференциальные свойства S-блоков замены для алгоритма ГОСТ 28147-89 // Инженерный вестник Дона. – 2015. – № 4. – http://ivdon.ru/ru/magazine/archive/n4y2015/3284.

18. *Красовский А.В.* Теоретическая атака на полный шифр Кузнечик со связанными ключами // Материалы VII Всероссийской молодежной школы-семинара по проблемам информационной безопасности «Перспектива-2016». – Таганрог: Изд-во ЮФУ, 2016. – С. 135-144.
19. *Ищукова Е.А., Алексеев Д.М.* Алгоритм анализа шифра Магма с использованием метода слайдовой атаки // Научное периодическое издание «CETERIS PARIBUS». – 2015. – № 5 (5). – С. 24-27. – http://efir-msk.ru/sbornik/%D0%A1%D0%A05.pdf.
20. *Ищукова Е.А., Алексеев Д.М.* Использование технологии MPI для анализа алгоритма шифрования Магма // Сборник трудов XIII Всероссийской научной конференции молодых ученых, аспирантов и студентов, г. Таганрог, 2015 г. – Ростов-на-Дону: Изд-во ЮФУ, 2016 – Т. 3. – С. 234-247.

REFERENCES

1. Kriptograficheskaya zashchita informatsii. Blochnye shifry [Cryptographic protection of information. Block ciphers]. Available at: https://www.tc26.ru/standard/gost/GOST_R_3412-2015.pdf.
2. *Babenko L.K. Ishchukova E.A. Sidorov I.D.* Parallel'nye algoritmy dlya resheniya zadach zashchity informatsii [Parallel algorithms for solving problems of information security]. Moscow: Goryachaya liniya Telekom, 2014, 304 p.
3. *Babenko L.K., Ishchukova E.A., Lomov I.S.* Matematicheskoe modelirovanie kriptograficheskogo algoritma «Kuznechik» [Mathematical modeling of a cryptographic algorithm "Grasshopper"], *Informatsionnoe protivodeystvie ugrozam terrorizma* [Information counteraction to the terrorism threats], 2015, pp. 166-176.
4. *Biryukov A., Vagner D.* Slaydovye ataki [Slide attacks], *Trudy bystrogo programmnogo shifrovaniya. Lektsii v oblasti komp'yuternykh nauk* [Proceedings of fast software encryption. Lectures in computer science], 1999, No. 1636, pp. 245-259.
5. *Biryukov A., Vagner D.* Rasshirennaya slaydovaya ataka. Dostizheniya v kriptologii [Advanced slide attack. Advances in cryptology], *Evrokript. Lektsii v oblasti komp'yuternykh nauk* [Eurocrypt. Lectures in computer science], 2000, No. 1807, pp. 589-606.
6. *Matsui M.* Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology – EUROCRYPT'93, Springer-Verlag, 1998, 386 p.
7. *Babenko L.K., Ishchukova E.A.* Sovremennye algoritmy blochnogo shifrovaniya i metody ikh analiza [Modern block encryption algorithms and methods of their analysis]. Moscow: Gelios ARV, 2006, 376 p.
8. *Biham E., Biryukov A., Shamir A.* Cryptanalysis of Skipjack Reduced to 31 Rounds using Impossible Differentials, *Advances in Cryptology - EUROCRYPT '99*. Prague: Springer-Verlag, pp. 12-23.
9. *Raphael C.-W. Phan*. Impossible Differential Cryptanalysis of Mini-AES, *Cryptologia*, October 2003, No. XXVII (4), pp. 283-292.
10. *Raphael C.-W. Phan, Mohammad Umar Siddiqi* Generalised Impossible Differentials of Advanced Encryption Standard, *Electronics Letters*, July 2001, No. 37 (14), pp. 896-898.
11. *Pis'menskiy M.V., Ishchukova E.A.* Kriptoanaliz S-AES s pomoshch'yu metoda nevozmozhnykh differentsialov [Cryptanalysis of S-AES using the method of impossible differentials], *«Studencheskiy nauchnyy forum» - 2016. Aktual'nye problemy informatsionnoy bezopasnosti* ["Student's scientific forum" in 2016. Actual problems of information security]. Available at: http://www.scienceforum.ru/2016/pdf/24173.pdf.
12. *Eli Biham, Orr Dunkelman, and Nathan Keller.* New results on boomerang and rectangle attacks, *In FSE'02.* Springer, 2002, Vol. 2365 of LNCS.
13. *Eli Biham, Orr Dunkelman, and Nathan Keller.* Related-key boomerang and rectangle attacks, *In EUROCRYPT'05.* Springer, 2005, Vol. 3494 of LNCS, pp. 507-525.
14. *Biryukov A., Khovratovich D., and Iv. Nikoli´c.* Examples of differential multicollisions for 13 and 14 rounds of AES-256, 2009. Available at: http://eprint. iacr.org/2009/242.pdf.
15. *Rudskoy V.* On zero rractical significance of "key recovery attack on full GOST block cipher with zero time and memory", 2010. Available at: http://eprint.iacr.org/2010.
16. *Pudovkina M.A., Khoruzhenko G.I.* Ataka na shifrsistemu GOST 28147-89 s 12 svyazannymi klyuchami [The attack on simsystem GOST 28147-89 with 12 related keys], *Matematicheskie voprosy kriptografiii* [Mathematical problems kriptografii], 2013, Vol. 4, Issue 2, pp. 127-152.

17. *Ishchukova E.A., Kalmykov I.A.* Differentsial'nye svoystva S-blokov zameny dlya algoritma GOST 28147-89 [Differential properties of S-block replacement algorithm GOST 28147-89], *Inzhenernyy vestnik Dona* [Engineering journal of Don], 2015, No. 4. Available at: http://ivdon.ru/ru/magazine/archive/n4y2015/3284.
18. *Krasovskiy A.V.* Teoreticheskaya ataka na polnyy shifr Kuznechik so svyazannymi klyuchami [A theoretical attack on the full cipher Grasshopper with associated keys], *Materialy VII Vserossiyskoy molodezhnoy shkoly-seminara po problemam informatsionnoy bezopasnosti «Perspektiva-2016»* [Proceedings of the VII all-Russian youth school-seminar on problems of information security "Perspective-2016"]. Taganrog: Izd-vo YuFU, 2016, pp. 135-144.
19. *Ishchukova E.A., Alekseev D.M.* Algoritm analiza shifra Magma s ispol'zovaniem metoda slaydovoy ataki [The analysis algorithm of the cipher Magma using the slide attack], *Nauchnoe periodicheskoe izdanie «CETERIS PARIBUS»* [Scientific periodical "CETERIS PARIBUS"], 2015, No. 5 (5), pp. 24-27. Available at: http://efir-msk.ru/sbornik/%D0%A1%D0%A05.pdf.
20. *Ishchukova E.A., Alekseev D.M.* Ispol'zovanie tekhnologii MPI dlya analiza algoritma shifrovaniya Magma [The use of MPI technology for the analysis of the encryption algorithm of Magma], *Sbornik trudov XIII Vserossiyskoy nauchnoy konferentsii molodykh uchenykh, aspirantov i studentov, g. Taganrog, 2015 g.* [Proceedings of the XIII all-Russian scientific conference of young scientists, postgraduates and students, Taganrog, 2015]. Rostov-na-Donu: Izd-vo YuFU, 2016, Vol. 3, pp. 234-247.

Статью рекомендовал к опубликованию д.т.н., профессор К.Е. Румянцев.

Бабенко Людмила Климентьевна – Южный федеральный университет; e-mail: blk@fib.tsure.ru; 347928, г. Таганрог, ул. Чехова, 2; тел.: 88634312018; кафедра безопасности информационных технологий; профессор.

Ищукова Евгения Александровна – e-mail: jekky82@mail.ru; тел.: 88634371905; кафедра безопасности информационных технологий; доцент.

Алексеев Дмитрий Михайлович – e-mail: jekky82@mail.ru; кафедра безопасности информационных технологий; студент.

Красовский Андрей Ваильевич – e-mail: an.krasowsckij@gmail.com; кафедра безопасности информационных технологий; студент.

Письменский Максим Владимирович – e-mail: makspismensky1@gmail.ru; кафедра безопасности информационных технологий; студент.

Babenko Lyudmila Klimentevna – Southern Federal University; e-mail: blk@fib.tsure.ru; 2, Chehov street, Taganrog, 347928, Russia; phone: +78634312018; the department of security of information technologies; professor.

Ishchukova Evgeniya Aleksandrovna – e-mail: jekky82@mail.ru; phone: +78634371905; the department of security of information technologies; associate professor.

Alekseev Dmitry Mikhailovich – e-mail: jekky82@mail.ru; the department of security of information technologies; student.

Krasovskiy Andrey Vasilievich – e-mail: an.krasowsckij@gmail.com; the department of security of information technologies; student.

Pismenskiy Maxim Vladimirovich – e-mail: makspismensky1@gmail.ru; the department of security of information technologies; student.