ОСОБЕННОСТИ ПРИМЕНЕНИЯ МЕТОДОВ ЛИНЕЙНОГО И ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА К СИММЕТРИЧНЫМ БЛОЧНЫМ ШИФРАМ

***Бабенко Людмила Климентьевна**, доктор технических наук, профессор, г. Таганрог*
***Ищукова Евгения Александровна**, кандидат технических наук, г. Таганрог*

В статье рассматриваются основные этапы оценки стойкости современных симметричных блочных шифров с использованием методов дифференциального и линейного криптоанализа. Определены основные этапы проведения каждого вида анализа. Рассмотрена возможность применения распределенных многопроцессорных вычислений. Кратко описаны особенности программной реализации различных этапов анализа. Приведены результаты экспериментов, полученные на основе использования разработанных и реализованных алгоритмов.

***Ключевые слова**: криптография, криптоанализ, секретный ключ, блочный шифр, стойкость, распределенные многопроцессорные вычисления, линейный криптоанализ, дифференциальный криптоанализ.*

APPLICATION FEATURES OF LINEAR AND DIFFERENTIAL CRYPTANALYSIS METHODS TO SYMMETRIC BLOCK CIPHER

***Ludmila Babenko**, Doctor of Science (Tech), Professor, Taganrog*
***Evgeniya Ischukova**, Ph.D., Taganrog*

The main stages of evaluation of modern symmetric block cipher resistance using the methods of differential and linear cryptanalysis are considered in the article. The main stages of each type of analysis are given. The possibility of using distributed multiprocessor computing is given. Briefly described the features of the software implementation of the various stages of analysis. Experimental results obtained through the use of developed and implemented algorithms are given.

***Keywords**: cryptography, cryptanalysis, secret key, block cipher, strength, distributed multiprocessing, linear cryptanalysis, differential cryptanalysis.*

Современная криптография основана на понятии односторонней функции $y = f_k(x)$, которая обладает следующим важным свойством: зная x и k легко вычислить значение y, но при этом вычислительно сложно определить значение x, зная только y. Стойкость современных шифров, помимо собственно алгоритма шифрования, во многом определяется длиной используемого ключа шифрования. Современная криптография исходит из того, что секретность шифра обеспечивается исключительно ключом шифрования, так как сам алгоритм рано или поздно может стать известным противнику [1].

В настоящей работе мы постараемся осветить наиболее характерные особенности современных криптографических систем, а также рассмотрим основные проблемы, связанные с определением криптографической стойкости современных систем защиты информации, и подходы к их решению.

Симметричное шифрование, которое в литературе еще называют традиционным шифрованием или шифрованием с одним ключом, до изобретения шифрования с открытым ключом было единственным методом шифрования. Шифрование с открытым ключом впервые было описано в откры-

той литературе в 1976 году, когда в США был утвержден стандарт шифрования данных DES (Data Encryption Standard) [2]. Этот стандарт использовался довольно длительное время (более 20 лет) пока в 2001 году не был принят новый стандарт AES (Advanced Encryption Standard), в основу которого лег алгоритм шифрования Rijndael. В России же официальным государственным стандартом является алгоритм шифрования ГОСТ 28147-89.

Для симметричных алгоритмов шифрования характерны следующие свойства:

- использование одного и того же алгоритма как для зашифрования, так и для расшифрования данных;

- использование одного ключа, который является секретным.

Современные симметричные алгоритмы шифрования разделяются на блочные и поточные. Для блочных алгоритмов шифрование информации производится небольшими порциями –блоками; как правило размер блока кратен 32 битам и составляет 64, 128, 192 или 256 битов. К современным алгоритмам симметричного шифрования относятся такие шифры как: DES, AES (Rijndael), RC5, ГОСТ 28147-89 и многие другие. Подробное описание многих современных симметричных алгоритмов шифрования можно найти в монографии авторов настоящей статьи «Современные алгоритмы шифрования и методы их анализа» [3]. Кроме того в 2009 году вышла книга С. Панасенко, представляющая собой довольно подробный справочник по симметричным системам шифрования, в котором описано более 50 алгоритмов шифрования [4].

Поточные шифры обычно шифруют информацию в режиме реального времени, как правило, побитно (реже побайтно) и используют для шифрования специально вырабатываемую псевдослучайную последовательность. К поточным шифрам, например, относится широко известный шифр A5/1, который используется для шифрования связи GSM (Group Special Mobile – мобильная групповая специальная связь). На сегодняшний день имеется достаточно большое число различных поточных шифров. Только в книге «Поточные шифры», вышедшей в 2003 году описано более 20 шифров [5].

В настоящий момент выделяют два основных способа построения симметричных алгоритмов шифрования: схему Фейстеля и сеть на основе подстановок и перестановок (SPN – Substitution-Permutation Network). По схеме Фейстеля построены алгоритмы DES, RC5, ГОСТ 28147-89 и др. Самым ярким представителем использования сети SPN является стандарт AES.

Ключевой задачей защиты информации является создание стойких алгоритмов шифрования. Любой конструируемый алгоритм подвергается тщательному анализу с целью выявления его слабых мест и возможности взлома. Алгоритм является относительно стойким до тех пор, пока не будут обнаружены методы и пути его анализа, позволяющие получить секретный ключ шифрования значительно быстрее, чем это можно сделать с использованием метода «грубого перебора». Рассмотрим основные известные на сегодняшний момент методы анализа симметричных систем.

Дифференциальный криптоанализ

Метод дифференциального криптоанализа впервые был предложен в начале 90-х годов прошлого века Э. Бихамом и А. Шамиром для анализа алгоритма шифрования DES. Хотя в книге Б. Шнайера [6] упоминается о том, что разработчики алгоритма DES знали о возможности такого анализа еще во время разработки алгоритма в 70-х годах XX века, широкая общественность узнала о дифференциальном криптоанализе именно из работ [7, 8]. Метод ДК оказался первым методом, позволяющим взломать DES при оценке сложности задач менее 2^{55}. Согласно [7], с помощью данного метода можно провести криптоанализ DES при усилиях порядка 2^{37}, но при наличии 2^{47} вариантов избранного открытого текста. Хотя 2^{47}, очевидно, значительно меньше, чем 2^{55}, необходимость при этом иметь 2^{47} вариантов избранного открытого текста превращает данный вариант схемы криптоанализа в чисто теоретическое упражнение [9]. Это связано с тем, что метод ДК был известен в момент разработки DES, но засекречен по очевидным соображениям, что подтверждается публичными заявлениями самих разработчиков [6]. В работе [8] показано, что если поменять порядок следования блоков замены в алгоритме шифрования DES или использовать другие наборы таблиц подстановок и перестановок, то алгоритм становится сразу намного слабее и может быть взломан менее чем за половину времени, требуемой для анализа алгоритма DES с помощью полного перебора. Это показывает значимость знания возможных путей анализа разрабатываемого алгоритма.

С помощью метода дифференциального криптоанализа (differential cryptanalysis), предложенного Э.Бихамом и А.Шамиром [7, 8], сложность анализа сократилась до 2^{37}. Однако при этом для проведения анализа необходимо было иметь 2^{37} особым образом подобранных текстов, зашифро-

ванных на одном и том же секретном ключе. Не смотря на накладываемые ограничения в использовании новых предложенных методов анализа – это был прорыв! Дальнейшее развитие этого метода показало возможность его применения к целому классу различных видов шифров, позволило выявить слабые места многих используемых и разрабатываемых алгоритмов шифрования. Сегодня этот метод, а также некоторые его производные, такие как метод линейно-дифференциальный, метод невозможных дифференциалов, метод бумеранга широко используются для оценки стойкости вновь создаваемых шифров. Именно поэтому специалисту по защите информации необходимо иметь представление о механизмах анализа шифров с использованием современных методов криптоанализа.

Само название дифференциальный криптоанализ происходит от английского слова difference, то есть разность. Именно поэтому в отечественной литературе этот вид анализа еще иногда называют разностным методом. Исходя из названия, можно понять, что при рассмотрении возможности анализа некоторого блочного алгоритма шифрования ученым пришло в голову использовать не отдельные тексты, а пары текстов. Понятно, что два текста будут иметь различия в некоторых позициях. Для того, чтобы определить это различие, достаточно пару текстов сложить между собой по модулю два. Результат такого сложения даст на выходе значение 0 в тех позициях, в которых исходные тексты были равны между собой, и соответственно значение 1 в тех позициях, в которых исходные тексты отличались. Например, рассмотрим два 4-битовых сообщения: $X = 0011$ и $X' = 1010$. В результате сложения текстов X и X' была получена разность $\Delta X = 1001$, полученное значение ΔX принято называть дифференциалом или разностью. В дифференциальном криптоанализе значение разности (дифференциала) принято обозначать символом Δ. Разность, полученная в результате сложения текстов X и X' показывает, что во второй и третьей позициях исходные сообщения X и X' были равны, а в первой и четвертой отличались друг от друга.

Здесь целесообразно будет ввести несколько определений, характерных для метода дифференциального криптоанализа, которыми мы будем оперировать в дальнейшем. Для большей наглядности основные значения пояснены с помощью рис. 1

В общем виде дифференциальный анализ блочных алгоритмов шифрования сводится к следующим основным пунктам:

1. Нахождение для алгоритма шифрования характеристик, обладающих максимальными характеристиками. Поиск характеристик ведется на основе дифференциальных свойств нелинейных криптографических примитивов, входящих в состав алгоритма шифрования.

2. Поиск правильных пар текстов с использованием найденных характеристик.

3. Анализ правильных пар текстов и накопление статистики о возможных значениях секретного ключа шифрования.

Первый пункт, заключающийся в поиске лучших характеристик для большинства алгоритмов, выполняется единожды и является теоретической задачей. Значения характеристик полностью зависят от структуры алгоритма шифрования и используемых криптографических примитивов. Иначе дело обстоит лишь с теми алгоритмами, которые обладают нефиксированными элементами. К таким алгоритмам можно, например, отнести алгоритм шифрования ГОСТ 28147-89, у которого S-блоки замены могут выбираться произвольным образом. Для таких алгоритмов поиск характеристик необходимо каждый раз начинать сначала, основываясь на дифференциальных свойствах выбранных S-блоков. Для автоматизации процесса анализа можно разработать алгоритм поиска лучших характеристик, основываясь на алгоритмах поиска по дереву. Для таких алгоритмов можно использовать параллельные модели для ускорения поиска характеристик.

Второй шаг анализа является вычислительно стойкой задачей для любого алгоритма шифрования, при этом не важно, обладает он фиксированными или нефиксированными элементами. Анализ заключается в опробовании большого числа пар текстов с целью определения правильной пары текстов, то есть той парой текстов, которую в дальнейшем можно использовать для анализа с целью поиска секретного ключа шифрования. Данный шаг может и должен быть легко представим в виде параллельных вычислений для сокращения времени анализа [12, 13, 15, 16].

Последний шаг легко реализуем, требует гораздо меньше вычислений в сравнении со вторым шагом. Он может быть реализован как отдельно в виде последовательного алгоритма, так и быть включенным в состав параллельных алгоритмов по поиску правильных пар текстов. В последнем случае при нахождении правильной пары текстов сразу можно провести ее анализ по накоплению статистики о возможном значении секретного ключа.

На кафедре БИТ ЮФУ исследования в области дифференциального криптоанализа ведутся с 2003 года. За это время получено множество результатов, которые нашли отражение в большом числе публикаций. Среди них отдельно можно выделить следующие.

На основе метода дифференциального криптоанализа, предложенного Э. Бихамом и А. Шамиром, разработаны последовательные алгоритмы поиска правильных пар текстов по заданному дифференциалу и секретного ключа для проведения анализа n-раундового (n≤16) алгоритма DES. Проведен анализ 6 раундов алгоритма DES с использованием наиболее вероятных значений дифференциалов [10 – 13]. Показано, что на 2-процессорной системе с частотой процессоров 1,41 ГГц время анализа в среднем составляет 7,5 минут, на 16-процессорной – 56 секунд. Проведен полный анализ диапазона входных разностей для алгоритма DES, состоящего из 8, 10, 12, 14 и 16 раундов на m-процессорном кластере (m≤16) с использованием разработанной методики. Показано, что при увеличении числа процессоров наблюдается практически линейный рост ускорения времени анализа. Кроме того, показано, что процент текстов, полностью соответствующих схеме преобразования заданного дифференциала, от общего числа найденных правильных пар текстов, лежит в диапазоне от 80% до100%, что гарантирует успех анализа. Проведен анализ 16-раундового алгоритма DES с использованием 16-процессорного кластера (частота 1,41 ГГц). Показано, что время работы программы составило 24 часа 13 минут.

Разработан рекурсивный алгоритм поиска дифференциалов, обладающих максимальной вероятностью, для алгоритма шифрования ГОСТ 28147-89, учитывающего различные варианты заполнения для блоков замены, для отбора правильных пар текстов при дальнейшем анализе [14 – 18]. На его основе разработан параллельный алгоритм поиска наиболее вероятных дифференциалов для алгоритма ГОСТ 28147-89 с учетом статического и динамического распределения данных и межпроцессорных взаимодействий при выявлении дифференциала с максимальной вероятностью. Проведены тестовые испытания анализа алгоритма шифрования ГОСТ 28147-89 для различных сочетаний следующих параметров: числа раундов шифрования, начального значения пороговой вероятности, количества процессоров, способа распределения данных. Показано, что при задании ненулевого значения пороговой вероятности, скорость вычислений в среднем возрастает в 1,285 раз. Показано, что при использовании 16 процессоров для анализа со статическим распределением данных время вычислений сокращается в 2,88 раза, а с динамическим – в 4,4 раза по сравнению с такими же расчетами на двухпроцессорной системе. Показано, что для алгоритма с динамическим распределением данных до 8 процессоров наблюдается линейный рост ускорения.

Для алгоритма ГОСТ 28147-89 показано, что существует ряд S-блоков, обладающих слабыми свойствами по отношению к дифференциальному криптоанализу [19 – 22]. Использование таких блоков в алгоритме ГОСТ позволяет получать характеристики, обладающие довольно высокими вероятностями, которые можно использовать для проведения атаки. Так, при использовании одного и того же слабого блока замены, вероятность характеристики для 32 раундов ГОСТ может составлять 2-25, что позволяет сравнительно легко получать правильные пары текстов для анализа. Для подтверждения предположений была осуществлена атака на 12 раундов алгоритма ГОСТ, которая за несколько минут позволяет определить первый раундовый подключ шифрования.

Разработан параллельный алгоритм проведения дифференциального анализа алгоритма Rijndael, лежащего в основе стандарта шифрования данных AES, с учетом межпроцессорного распределения данных и взаимодействия процессов при нахождении ключа шифрования [23].

Рассмотрена возможность применения метода дифференциального криптоанализа к анализу поточных шифров [24] и современных функций хэширования [25].

Дополнительные сведения о дифференциальном криптоанализе можно найти в статьях [26 - 29], монографиях [3, 29] и учебном пособии [30].

Линейный криптоанализ

Метод линейного криптоанализа впервые был предложен в начале 90-х годов XX века японским ученым М. Матсуи (Matsui). В своей работе [31] М. Матсуи показал, как можно осуществить атаку на алгоритм шифрования DES, сократив сложность анализа до 2^{47}. Существенным недостатком метода стала необходимость иметь в наличии большой объем данных, зашифрованных на одном и том же секретном ключе, что делало метод малопригодным для практического применения к вскрытию шифра. Однако, если предположить, что к аналитику в руки попал шифрованный текст, содержащий важные сведения, а также некий черный ящик (устройство или программа), который позволяет

выполнить любое число текстов, зашифрованных с помощью известного алгоритма шифрования на секретном ключе, не раскрывая при этом самого ключа, то применение метода линейного криптоанализа становится вполне реальным. Многие алгоритмы шифрования, известные на момент опубликования работы [31], впоследствии были проверены на устойчивость к этому методу и не все из них оказались достаточно стойкими и, как следствие, потребовали доработки.

Любой алгоритм шифрования в самом общем виде можно представить как некоторую функцию E, зависящую от входного сообщения X, секретного ключа K и возвращающую шифрованное сообщение Y:

$$Y = E(X, K) \quad (1)$$

Зная само преобразование E и входное сообщение X, нельзя однозначно сказать каким будет выходное сообщение Y. В данном случае нелинейность функции зависит от внутренних механизмов преобразования E и секретного ключа K. М. Матсуи показал, что существует возможность представить функцию шифрования в виде системы уравнений, которые выполняются с некоторой вероятностью p. При этом для успешного проведения анализа вероятность уравнений p должна быть как можно дальше удалена от значения 0,5.

Так как уравнения, получаемые в ходе анализа криптоалгоритма, являются вероятностными, то их называют линейными статистическими аналогами. Линейным статистическим аналогом нелинейной функции шифрования (1) называется величина Q, равная сумме по модулю двух скалярных произведений входного вектора X, выходного вектора Y и вектора секретного ключа K соответственно с двоичными векторами γ, β и α, имеющими хотя бы одну координату равную единице:

$$Q = (X, \gamma)\ \alpha\ (Y, \beta) \oplus (K, \oplus)$$

в том случае, если вероятность того, что Q=0 отлична от 0,5 ($P(Q=0)\neq 0,5$).

В отличие от дифференциального криптоанализа, в котором большое значение вероятности гарантировало успех атаки, в линейном криптоанализе успех анализа может быть обеспечен как уравнениями с очень большой вероятностью, так и уравнениями с очень маленькой вероятностью. Для того, чтобы понять, какое из возможных уравнений лучше всего использовать для анализа, используют отклонения. Отклонением линейного статистического аналога называют величину

$$\eta = |1 - p|$$

где p – вероятность, с которой выполняется линейный аналог.

Отклонение определяет эффективность линейного статистического аналога. Чем отклонение больше, тем выше вероятность успешного проведения анализа. Фактически отклонение показывает насколько вероятность статистического аналога отдалена от значения p = 0,5.

Для успешного применения метода линейного криптоанализа необходимо решить следующие задачи. Найти максимально эффективные (или близкие к ним) статистические линейные аналоги. При нахождении аналогов обратить внимание на то, что в них должно быть задействовано как можно больше битов искомого секретного ключа K. 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.

Первый шаг анализа заключается в нахождении эффективных статистических аналогов. Для алгоритмов шифрования, в которых все блоки заранее известны, этот шаг можно выполнить единожды, основываясь на анализе линейных свойств всех криптографических элементов шифра. Для алгоритма ГОСТ 28147-89 такой подход неприемлем, в связи с использованием нефиксированных S-блоков. То есть данный этап анализа каждый раз при смене используемых S-блоков необходимо повторять сначала. В результате анализа должна быть получена система уравнений, выполняющихся с некоторыми вероятностями. Левая часть уравнений должна содержать в себе сумму битов входного и выходного сообщения, правая часть уравнения – биты секретного ключа. Если первый шаг анализа является чисто теоретическим и полностью зависит от структуры алгоритма, то второй шаг – является исключительно практической частью, которая заключается в анализе известных пар открытый-закрытый текст с помощью полученной ранее системы статистических аналогов. Для этого используется следующий алгоритм.

Алгоритм. Пусть N – число всех открытых текстов и T – число открытых текстов, для которых левая часть линейного статистического аналога равна 0. Рассмотрим два случая.

Таблица 1

Слабый блок замены, определенный в результате работы предложенного алгоритма

Вход	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Выход	15	7	11	3	13	5	9	1	14	6	10	2	12	4	8	0

Если $T > N/2$, то в этом случае число открытых текстов, для которых левая часть аналога равна нулю, больше половины, то есть в большинстве случаев в левой части аналога появляется значение, равное нулю, то

- если вероятность этого линейного статистического аналога $p > 1/2$, это говорит о том, что в большинстве случаев правая и левая части аналога равны, а значит левая часть аналога, содержащая биты ключа, равна 0.

- если вероятность этого линейного статистического аналога $p < 1/2$, это говорит о том, что в большинстве случаев правая и левая части аналога не равны, а значит левая часть аналога, содержащая биты ключа, равна 1.

2. Если $T < N/2$, то в этом случае число открытых текстов, для которых левая часть аналога равна нулю, меньше половины, то есть в большинстве случаев в левой части аналога появляется значение, равное единице, то

- если вероятность этого линейного статистического аналога $p > 1/2$, это говорит о том, что в большинстве случаев правая и левая части аналога равны, а значит левая часть аналога, содержащая биты ключа, равна 1.

- если вероятность этого линейного статистического аналога $p < 1/2$, это говорит о том, что в большинстве случаев правая и левая части аналога не равны, а значит левая часть аналога, содержащая биты ключа, равна 0.

На основе проведенного исследования был разработан алгоритм оценки надежности блока замены по отношению к линейному криптоанализу. Для ускорения времени анализа предложено использовать параллельную структуру, позволяющую каждому процессору производить независимую обработку различных заполнений S-блока. Для оптимизации предложенных алгоритмов введена классификация уровней стойкости используемых блоков замены. Показано, что первый этап анализа может быть автоматизирован для алгоритмов шифрования, не обладающих устойчивой структурой. Таких как, например, алгоритм ГОСТ 28147-89, для которого изменение заполнения блоков замены влечет за собой необходимость построения новой системы уравнений. В результате проведенного исследования и при использовании предложенной классификации, был получен универсальный инструмент для быстрого определения полного списка слабых блоков по отношению к линейному криптоанализу. Работа разработанного алгоритма поиска слабых блоков была опробована на примере анализа блоков замены для алгоритма шифрования ГОСТ 28147-89. Применение разработанного алгоритма позволило без труда обнаружить большое число ослабленных блоков замены, использование которых может значительно ослабить стойкость используемого алгоритма шифрования. Полный анализ выполняется в течение нескольких минут (все исследования проводились на процессоре Intel Celeron M CPU 530 1.73 GHz, RAM 1007Mb). Мы попробовали варьировать критерий слабого блока по минимальному количеству экстремумов, которое необходимо найти. Более подробное описание можно найти в работах [32 – 35].

Для примера на рис. 2 и 3 представлена схема построения линейного аналога для 8-раундового алгоритма шифрования. Жирным выделены связи, используемые для этого. Для блока замены, представленного в табл. 1, полученный линейный аналог будет иметь вид:

$$PR[32] \gamma PL[18] \oplus CR[29] \oplus CR[18] \oplus CL[32] \oplus CR[21] \oplus CL[12] = K1[32] \oplus K3[32] \oplus K4[10] \oplus K5[32] \oplus K5[10] \oplus K6[29] \oplus K7[12] \oplus K7[32] \oplus K7[24] \oplus K8[10] \oplus K8[21] \ (p=0)$$

При рассмотрении вопросов анализа особое внимание уделялось возможности применения распределенных многопроцессорных вычислений для сокращения времени анализа. В ходе тестовых экспериментов проводились замеры скорости вычислений для разных начальных условий: числа процессоров, участвующих в вычислениях, количества раундов шифрования и начального значения пороговой вероятности. В условиях реального времени удалось получить результаты для 16-раундового алгоритма шифрования ГОСТ 28147-89. Экспериментально было показано, что эффективность применения разработанных алгоритмов зависит не только от числа используемых процессоров и количества раундов шифрования, но и от способа распределения данных анализа.

Литература:

1. Шеннон К., Теория связи в секретных системах // http://www.enlight.ru/crypto/articles/shannon/shann__i.htm
2. Е.Б Маховенко, Теоретико-числовые методы в криптографии: Учебное пособие. – М.:Гелиос АРВ, 2006. – 320 с.
3. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа – Москва, «Гелиос АРВ», 2006. – 376 с.
4. Панасенко С., Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.
5. Асосков А.В., Иванов М.А., Мирский А.А., Рузин А.В., Сланин А.В., Тютвин А.Н. Поточные шифры – М.: КУДИЦ-ОБРАЗ, 2003.-336с.
6. Шнайер Б., Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си – М.:ТРИУМФ,2002. – С. 648.
7. Biham E., Shamir A., Differential Cryptanalysis of the Full 16-round DES, Crypto'92, Springer-Velgar, 1998, p.487
8. Biham E., Shamir A., Differential Cryptanalysis of DES-like Cryptosystems, Extended Abstract, Crypto'90, Springer-Velgar, 1998, p.2
9. Столлингс В., Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М,: Издательский дом «Вильямс», 2001.
10. Бабенко Л.К. Мишустина (Ищукова) Е.А. Применение методов криптоанализа для исследования стойкости современных блочных шифров // Тезисы докладов X всероссийской научной конференции. "Проблемы информационной безопасности в системе высшей школы", М.: МИФИ, 2003.
11. Бабенко Л.К. Ищукова Е.А. Параллельная реализация метода дифференциального криптоанализа // Материалы VI Международной научно-практической конференции «Информационная безопасность», Таганрог: ТРТУ, 2004.
12. Ищукова Е.А. Дифференциальный криптоанализ алгоритма шифрования DES с использованием распределенных вычислений // VII Всероссийская научная конференция студентов и аспирантов «Техническая кибернетика, радиоэлектроника и системы управления», Таганрог: Изд-во ТРТУ, 2006 г., с. 340 – 341.
13. Babenko L.K., Ishchukova E.A. Data Distribution Algoritms for Differential Cryptanalysis of DES // Proceeding of the Workshop on Computer Science and Information Technologies (CSIT'2007)? Krasnousolsk, UFA, September 13-16, 2007, Volume 1, UFA State Aviation Technical University, 2007 (198-201)
14. Ищукова Е.А. Применение рекурсивного алгоритма поиска в Б-деревьях для дифференциального криптоанализа алгоритма шифрования ГОСТ 28147-89 // Материалы IX Международной научно-практической конференции «Информационная безопасность». Часть 2. – Таганрог; Изд-во: ТТИ ЮФУ 2007 – С. 92-97.
15. Бабенко Л.К. Ищукова Е.А. Параллельный алгоритм поиска характеристик с максимальными вероятностями для дифференциального криптоанализа. // Многопроцессорные вычислительные и управляющие системы – 2007 // Материалы Международной научно-технической конференции. Т. 1 – Таганрог: Изд-во ТТИ
16. Бабенко Л.К. Ищукова Е.А. Дифференциальный криптоанализ блочных шифров с применением распределенных вычислений // Многопроцессорные вычислительные и управляющие системы – 2007 // Материалы Международной научно-технической конференции. Т. 1 – Таганрог: Изд-во ТТИ ЮФУ, 2007, с. 222 -227.
17. Ищукова Е.А., Бабенко Л.К. Поиск дифференциалов с максимальными вероятностями // Проблемы информатизации общества. Нальчик. – Изд-во КБНЦ РАН, 2008. – С. 115 – 120
18. Ищукова Е.А., Бабенко Л.К. Алгоритмы поиска дифференциалов с максимальными вероятностями для оценки криптографической стойкости блочных шифров методом дифференциального криптоанализа // Труды XXVI конференции «Мобильный бизнес»: Перспективы развития и проблемы реализации систем мобильной связи в России и за рубежом, Том I, октябрь 2008, о. Куба. – С. 32 – 44.
19. Ищукова Е.А. Исследование влияния блоков замены на устойчивость алгоритмов шифрования // Известия ЮФУ. Технические науки. – Таганрог: Изд-во ТТИ ЮФУ, 2008. – №8. – С. 210 – 215.
20. Дифференциальный криптоанализ алгоритма ГОСТ 28147-89 // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч.3. – Таганрог: Изд-во ТТИ ЮФУ, 2010.– С. 69 – 80.
21. Differential Analysis GOST Encryption Algorithm // Proceedings of the 3rd Internaternational Conference of Security of Information and Networks (SIN 2010), p.149-157, ACM, New York, 2010.
22. Бабенко Л.К., Ищукова Е.А. Дифференциальный криптоанализ алгоритма ГОСТ 28147-89 // Известия ЮФУ. Технические науки. Тематический выпуск. "Информационная безопасность". - Таганрог: Изд-во ТТИ ЮФУ, 20011. – С. 231 - 248.
23. Бабенко Л.К. Ищукова Е.А. Особенности дифференциального криптоанализа алгоритма AES // Известия ТРТУ 7. Тематический выпуск. Материалы VIII Международной научно-практической конференции «Информационная безопасность».– Таганрог, 3-7 июня. – С. 183-185.
24. Дифференциальный криптоанализ поточных шифров // Известия ЮФУ. – Технические науки. – Таганрог: Изд-во ТТИ ЮФУ, 2009. - №11. – С. 232 – 239
25. Дифференциальный криптоанализ упрощенной функции хэширования SHA // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ, 2010. - №11 (112). – С. 99 – 106

26. Бабенко Л.К. Мишустина (Ищукова) Е.А. Применение современных методов криптоанализа при проектировании скоростных блочных шифров // журнал «Телекоммуникации», М.: «Наука и технологии», 2003, №7
27. Принципиальные особенности проведения дифференциального криптоанализа блочных шифров // Известия ЮФУ. – Технические науки. – Таганрог: Изд-во ТТИ ЮФУ, 2009. - №11. – С. 221 – 232
28. Стойкость современных блочных шифров к методу дифференциального криптоанализа // Материалы XI Международной научно-практической конференции «Информационная безопасность». Ч.3. – Таганрог: Изд-во ТТИ ЮФУ, 2010.– С. 163 – 167
29. Бабенко Л.К., Ищукова Е.А. Анализ современных криптографических систем с помощью метода дифференциального криптоанализа // Актуальные аспекты защиты информации в Южном федеральном университете. Монография / Таганрог: Изд-во ТТИ ЮФУ, 2011. - С. 102 - 181.
30. Бабенко л.к., Ищукова Е.А. Учебное пособие по курсу «Криптографические методы и средства обеспечения информационной безопасности».– Таганрог: Изд-во ТТИ ЮФУ, 2011. – 148 с.
31. Matsui M., Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology – EUROCRYPT'93, Springer-Verlag, 1998, p.386.
32. L.K. Babenko, E.A.Ishchukova Influence of S-Boxes to the Resistance of GOST Algorithm against Linear Cryptanalysis // Proceedings of the 6th international conference on Security of information and networks (SIN 2013), ACM, New York, NY, USA, 352-355.
33. Бабенко Л.К., Ищукова Е.А. Использование слабых блоков замены для линейного криптоанализа блочных шифров // Известия Южного федерального университета. Технические науки. 2014. № 2 (151). С. 138-146.
34. Бабенко Л.К., Ищукова Е.А. Анализ алгоритма ГОСТ 28147-89: поиск слабых блоков // Известия Южного федерального университета. Технические науки. 2014. № 2 (151). С. 129-138.
35. Л.К. Бабенко, Е.А. Ищукова Линейный криптоанализ алгоритма ГОСТ 28147-89 // Материалы XIII Международной конференции «ИБ-2013». Ч. I. – Таганрог: Изд-во ЮФУ, 2013. - С. 226 - 235.

References:

1. Shennon K., Teorija svjazi v sekretnyh sistemah // http://www.enlight.ru/crypto/articles/shannon/shann__i.htm
2. E.B Mahovenko, Teoretiko-chislovye metody v kriptografii: Uchebnoe posobie. – M.:Gelios ARV, 2006. – 320 s.
3. Babenko L.K., Ishhukova E.A. Sovremennye algoritmy blochnogo shifrovanija i metody ih analiza – Moskva, «Gelios ARV», 2006. – 376 s.
4. Panasenko S., Algoritmy shifrovanija. Special'nyj spravochnik. – SPb.: BHV-Peterburg, 2009. – 576 s.
5. Asoskov A.V., Ivanov M.A., Mirskij A.A., Ruzin A.V., Slanin A.V., Tjutvin A.N. Potochnye shifry – M.: KUDIC-OBRAZ, 2003.-336s.
6. Shnajer B., Prikladnaja kriptografija: Protokoly, algoritmy, ishodnye teksty na jazyke Si – M.:TRIUMF,2002. – S. 648.
7. Biham E., Shamir A., Differential Cryptanalysis of the Full 16-round DES, Crypto'92, Springer-Velgar, 1998, p.487
8. Biham E., Shamir A., Differential Cryptanalysis of DES-like Cryptosystems, Extended Abstract, Crypto'90, Springer-Velgar, 1998, p.2
9. Stollings V., Kriptografija i zashhita setej: principy i praktika, 2-e izd.: Per. s angl. – M,: Izdatel'skij dom «Vil'jams», 2001.
10. Babenko L.K. Mishustina (Ishhukova) E.A. Primenenie metodov kriptoanaliza dlja issledovanija stojkosti sovremennyh blochnyh shifrov // Tezisy dokladov X vserossijskoj nauchnoj konferencii. "Problemy informacionnoj bezopasnosti v sisteme vysshej shkoly", M.: MIFI, 2003.
11. Babenko L.K. Ishhukova E.A. Parallel'naja realizacija metoda differencial'nogo kriptoanaliza // Materialy VI Mezhdunarodnoj nauchno-prakticheskoj konferencii «Informacionnaja bezopasnost'», Taganrog: TRTU, 2004.
12. Ishhukova E.A. Differencial'nyj kriptoanaliz algoritma shifrovanija DES s ispol'zovaniem raspredelennyh vychislenij // VII Vserossijskaja nauchnaja konferencija studentov i aspirantov «Tehnicheskaja kibernetika, radiojelektronika i sistemy upravlenija», Taganrog: Izd-vo TRTU, 2006 g., s. 340 – 341.
13. Babenko L.K., Ishchukova E.A. Data Distribution Algoritms for Differential Cryptanalysis of DES // Proceeding of the Workshop on Computer Science and Information Technologies (CSIT'2007)? Krasnousolsk, UFA, September 13-16, 2007, Volume 1, UFA State Aviation Technical University, 2007 (198-201)
14. Ishhukova E.A. Primenenie rekursivnogo algoritma poiska v B-derev'jah dlja differencial'nogo kriptoanaliza algoritma shifrovanija GOST 28147-89 // Materialy IH Mezhdunarodnoj nauchno-prakticheskoj konferencii «Informacionnaja bezopasnost'». Chast' 2. – Taganrog; Izd-vo: TTI JuFU 2007 – S. 92-97.
15. Babenko L.K. Ishhukova E.A. Parallel'nyj algoritm poiska harakteristik s maksimal'nymi verojatnostjami dlja differencial'nogo kriptoanaliza. // Mnogoprocessornye vychislitel'nye i upravljajushhie sistemy – 2007 // Materialy Mezhdunarodnoj nauchno-tehnicheskoj konferencii. T. 1 – Taganrog: Izd-vo TTI
16. Babenko L.K. Ishhukova E.A. Differencial'nyj kriptoanaliz blochnyh shifrov s primeneniem raspredelennyh vychislenij // Mnogoprocessornye vychislitel'nye i upravljajushhie sistemy – 2007 // Materialy Mezhdunarodnoj nauchno-tehnicheskoj konferencii. T. 1 – Taganrog: Izd-vo TTI JuFU, 2007, s. 222 -227.
17. Ishhukova E.A., Babenko L.K. Poisk differencialov s maksimal'nymi verojatnostjami // Problemy informatizacii obshhestva. Nal'chik. – Izd-vo KBNC RAN, 2008. – S. 115 – 120

18. Ishhukova E.A., Babenko L.K. Algoritmy poiska differencialov s maksimal'nymi verojatnostjami dlja ocenki kriptograficheskoj stojkosti blochnyh shifrov metodom differencial'nogo kriptoanaliza // Trudy HHVI konferencii «Mobil'nyj biznes»: Perspektivy razvitija i problemy realizacii sistem mobil'noj svjazi v Rossii i za rubezhom, Tom I, oktjabr' 2008, o. Kuba. – S. 32 – 44.
19. Ishhukova E.A. Issledovanie vlijanija blokov zameny na ustojchivost' algoritmov shifrovanija // Izvestija JuFU. Tehnicheskie nauki. – Taganrog: Izd-vo TTI JuFU, 2008. – №8. – S. 210 – 215.
20. Differencial'nyj kriptoanaliz algoritma GOST 28147-89 // Materialy XI Mezhdunarodnoj nauchno-prakticheskoj konferencii «Informacionnaja bezopasnost'». Ch.3. – Taganrog: Izd-vo TTI JuFU, 2010.– S. 69 – 80.
21. Differential Analysis GOST Encryption Algorithm // Proceedings of the 3rd Internaternational Conference of Security of Information and Networks (SIN 2010), p.149-157, ACM, New York, 2010.
22. Babenko L.K., Ishhukova E.A. Differencial'nyj kriptoanaliz algoritma GOST 28147-89 // Izvestija JuFU. Tehnicheskie nauki. Tematicheskij vypusk. «Informacionnaja bezopasnost'». - Taganrog: Izd-vo TTI JuFU, 20011. – S. 231 - 248.
23. Babenko L.K. Ishhukova E.A. Osobennosti differencial'nogo kriptoanaliza algoritma AES // Izvestija TRTU 7. Tematicheskij vypusk. Materialy VIII Mezhdunarodnoj nauchno-prakticheskoj konferencii «Informacionnaja bezopasnost'».– Taganrog, 3-7 ijunja. – S. 183-185.
24. Differencial'nyj kriptoanaliz potochnyh shifrov // Izvestija JuFU. – Tehnicheskie nauki. – Taganrog: Izd-vo TTI JuFU, 2009. - №11. – S. 232 – 239
25. Differencial'nyj kriptoanaliz uproshhennoj funkcii hjeshirovanija SHA // Izvestija JuFU. Tehnicheskie nauki. Tematicheskij vypusk «Informacionnaja bezopasnost'». – Taganrog: Izd-vo TTI JuFU, 2010. - №11 (112). – S. 99 – 106
26. Babenko L.K. Mishustina (Ishhukova) E.A. Primenenie sovremennyh metodov kriptoanaliza pri proektirovanii skorostnyh blochnyh shifrov // zhurnal «Telekommunikacii», M.: «Nauka i tehnologii», 2003, №7
27. Principial'nye osobennosti provedenija differencial'nogo kriptoanaliza blochnyh shifrov // Izvestija JuFU. – Tehnicheskie nauki. – Taganrog: Izd-vo TTI JuFU, 2009. - №11. – S. 221 – 232
28. Stojkost' sovremennyh blochnyh shifrov k metodu differencial'nogo kriptoanaliza // Materialy XI Mezhdunarodnoj nauchno-prakticheskoj konferencii «Informacionnaja bezopasnost'». Ch.3. – Taganrog: Izd-vo TTI JuFU, 2010.– S. 163 – 167
29. Babenko L.K., Ishhukova E.A. Analiz sovremennyh kriptograficheskih sistem s pomoshh'ju metoda differencial'nogo kriptoanaliza // Aktual'nye aspekty zashhity informacii v Juzhnom federal'nom universitete. Monografija / Taganrog: Izd-vo TTI JuFU, 2011. - S. 102 - 181.
30. Babenko L.K., Ishhukova E.A. Uchebnoe posobie po kursu "Kriptograficheskie metody i sredstva obespechenija informacionnoj bezopasnosti".– Taganrog: Izd-vo TTI JuFU, 2011. – 148 s.
31. Matsui M., Linear Cryptanalysis Method for DES Cipher, Advances in Cryptology – EUROCRYPT'93, Springer-Verlag, 1998, p.386.
32. L.K. Babenko, E.A.Ishchukova Influence of S-Boxes to the Resistance of GOST Algorithm against Linear Cryptanalysis // Proceedings of the 6th international conference on Security of information and networks (SIN 2013), ACM, New York, NY, USA, 352-355.
33. Babenko L.K., Ishhukova E.A. Ispol'zovanie slabyh blokov zameny dlja linejnogo kriptoanaliza blochnyh shifrov // Izvestija Juzhnogo federal'nogo universiteta. Tehnicheskie nauki. 2014. № 2 (151). S. 138-146.
34. Babenko L.K., Ishhukova E.A. Analiz algoritma GOST 28147-89: poisk slabyh blokov // Izvestija Juzhnogo federal'nogo universiteta. Tehnicheskie nauki. 2014. № 2 (151). S. 129-138.
35. L.K. Babenko, E.A. Ishhukova Linejnyj kriptoanaliz algoritma GOST 28147-89 // Materialy HIII Mezhdunarodnoj konferencii «IB-2013». Ch. I. – Taganrog: Izd-vo JuFU, 2013. - S. 226 - 235.