УДК 004.9
МРНТИ 81.96.00

https://doi.org/10.51889/2022-1.1728-7901.19

*Р.М. Оспанов[1], Е.Н. Сейткулов[1]**

[1] Евразийский национальный университет им. Л.Н.Гумилева, г. Нур-Султан, Казахстан
**e-mail: yerzhan.seitkulov@gmail.com*

МЕТОДЫ КРИПТОАНАЛИЗА И СВОЙСТВА S-БЛОКОВ

Аннотация

В работе рассматриваются методы криптоанализа и роль криптографических свойств S-блоков при проведении соответствующих атак. Симметричные криптографические преобразования обладают рядом преимуществ при практическом использовании с точки зрения их эффективности, скорости и надежности. При этом S-блоки играют важную роль в обеспечении стойкости симметричных преобразований. Для защиты алгоритмов от различных методов криптоанализа S-блоки должны обладать рядом криптографических свойств, удовлетворять ряду критериев. В настоящее время основными атаками, для которых имеют значения свойства S-блоков, используемых в криптографических алгоритмах, являются атаки, основанные на линейном, дифференциальном, алгебраическом методах криптоанализа. Другие методы анализа достаточно специфичны для отдельно взятого алгоритма, и, как правило, используют общую структуру алгоритма, а не отдельные его составляющие компоненты, как, например, S-блоки. В работе выполнен обзор существующих методов криптоанализа, использующих возможные слабости в S-блоках.

Ключевые слова*:* S-блоки, таблица замен, криптография, симметричное шифрование, защита информации.

Аңдатпа

Р.М. Оспанов[1], Е.Н. Сейтқұлов[1]
[1] Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан қ., Қазақстан

S-БЛОКТАРЫНЫҢ КРИПТО-ТАЛДАУ ӘДІСТЕРІ ЖӘНЕ ҚАСИЕТТЕРІ

Жұмыста криптоталдау әдістері және сәйкес шабуылдарды орындаудағы S-жәшіктерінің криптографиялық қасиеттерінің рөлі талқыланады. Симметриялық криптографиялық түрлендірулер тиімділігі, жылдамдығы және сенімділігі бойынша бірқатар практикалық артықшылықтарға ие. Бұл жағдайда S-блоктары симметриялық түрлендірулердің беріктігін қамтамасыз етуде маңызды рөл атқарады. Алгоритмдерді әртүрлі криптоталдау әдістерінен қорғау үшін S-блоктары бірқатар криптографиялық қасиеттерге ие болуы және бірқатар критерийлерді қанағаттандыруы керек. Қазіргі уақытта криптографиялық алгоритмдерде қолданылатын S-блоктарының қасиеттері маңызды болып табылатын негізгі шабуылдар сызықтық, дифференциалды, алгебралық криптоталдау әдістеріне негізделген шабуылдар болып табылады. Басқа талдау әдістері бір алгоритм үшін әбден спецификалық болып табылады және, әдетте, алгоритмнің S-блоктары сияқты жеке құрамдас бөліктерін емес, жалпы құрылымын пайдаланады. Қағаз S-блоктарындағы ықтимал әлсіздіктерді пайдаланатын қолданыстағы криптоталдау әдістерін қарастырады.

Түйін сөздер: S-блоктары, алмастыру кестесі, криптография, симметриялық шифрлау, ақпаратты қорғау.

Abstract

CRYPTO-ANALYSIS METHODS AND PROPERTIES OF S-BLOCKS

Ospanov R.M. [1], Seitkulov Ye.N.[1]
[1]Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan

The paper discusses cryptanalysis methods and the role of the cryptographic properties of S-boxes in carrying out the corresponding attacks. Symmetric cryptographic transformations have a number of practical advantages in terms of their efficiency, speed and reliability. In this case, S-boxes play an important role in ensuring the robustness of symmetric transformations. To protect algorithms from various cryptanalysis methods, S-boxes must have a number of cryptographic properties and satisfy a number of criteria. Currently, the main attacks for which the properties of S-boxes used in cryptographic algorithms are important are attacks based on linear, differential, algebraic cryptanalysis methods. Other analysis methods are quite specific for a single algorithm, and, as a rule, use the general structure of the algorithm, and not its individual components, such as S-boxes. The paper reviews existing cryptanalysis methods that exploit possible weaknesses in S-boxes.

Keywords: S-boxes, substitution table, cryptography, symmetric encryption, information protection.

1 Введение

Обеспечение свойств информационной безопасности таких, как конфиденциальность, целостность, целостность и т. д. обычно предполагает использование симметричного шифрования. Поскольку симметричные криптографические преобразования обладают рядом преимуществ при практическом использовании с точки зрения их эффективности, скорости и надежности. S-блоки играют важную роль в обеспечении стойкости симметричных преобразований. Для защиты алгоритмов от различных методов криптоанализа S-блоки должны обладать рядом криптографических свойств, удовлетворять ряду критериев.

В настоящее время основными атаками, для которых имеют значения свойства S-блоков, используемых в криптографических алгоритмах, являются атаки, основанные на линейном, дифференциальном, алгебраическом методах криптоанализа. Другие методы анализа достаточно специфичны для отдельно взятого алгоритма, и, как правило, используют общую структуру алгоритма, а не отдельные его составляющие компоненты, как, например, S-блоки. Далее рассмотрим ряд методов криптоанализа, и отметим роль свойств S-блоков при проведении соответствующих атак.

2 Основная часть

Дифференциальный криптоанализ. Одним из основных методов криптоанализа является дифференциальный криптоанализ. Свойство дифференциальной равномерности S-блока является показателем стойкости против дифференциальной атаки. Также для оценки стойкости против дифференциальной атаки используется таблица распределения разностей или XOR-таблица.

Дифференциальная атака использует неравномерное распределение выходных разностей, когда входные данные выбираются с фиксированной разницей. Хотя линейные компоненты в криптографических алгоритмах могут эффективно рассеивать различия, они не могут помочь уменьшить неравномерность в отношении разностей. Таким образом, равномерное дифференциальное распределение в основном исходит из нелинейных компонентов, таких как S-блоки.

Пусть $X' = [X1', X2', ..., Xn']$ и $X'' = [X1'', X2'', ..., Xn'']$ - n-битные входные данные шифра, где Xi' - i-й бит вектора X', Xi'' - i-й бит вектора X''. $\Delta X = X' \oplus X'' = [\Delta X1, \Delta X2, \ldots, \Delta Xn]$ - разность входных данных, где $\Delta Xi = Xi' \oplus Xi''$, «$\oplus$» - сложение по модулю 2 (побитовое исключающее ИЛИ (XOR)) для n-битных векторов.

Пусть $Y' = [Y1', Y2', ..., Yn']$ и $Y'' = [Y1'', Y2'', ..., Yn'']$ - соответствующие n-битные выходные данные шифра, где Yi' - i-й бит вектора Y', Yi'' - i-й бит вектора Y''. $\Delta Y = Y' \oplus Y'' = [\Delta Y1, \Delta Y2, \ldots, \Delta Yn]$ - это разность выходных данных, где $\Delta Yi = Yi' \oplus Yi''$.

Вероятность того, что определенная разность выходных данных ΔY возникает при определенной разности входных данных ΔX, в идеальном случае равна $1/2n$.

При дифференциальном криптоанализе используется случаи, в которых определенны конкретные разности выходных данных ΔY возникают при конкретных разности входных данных ΔX с очень большой вероятностью намного больше, чем $1/2n$.

Пары, состоящие из входных и соответствующих выходных разностей (ΔX, ΔY), называются дифференциалами. Дифференциальный криптоанализ относится к атакам по выбранному открытому тексту. Это означает, что при проведении такого вида атаки злоумышленник может выбирать входные данные и затем исследует выходные данные, пытаясь определить секретный ключ. При проведении дифференциальной атаки злоумышленник выясняет, что для определенного конкретного значения входной разности ΔX с высокой вероятностью встречается конкретное значение выходной разности ΔY, и выбирает пары входных данных X' и X'', удовлетворяющие это определенной разности ΔX. Оценка иммунитета против дифференциального криптоанализа является существенной при разработке безопасных блочных шифров.

Используя "wide trail design strategy" [1] можно легко посчитать сложность дифференциальной атаки на основе показателя дифференциальной равномерности S-блока.

Линейный криптоанализ. Следующий важный метод криптоанализа – линейный криптоанализ. Свойство нелинейности S-блока является показателем стойкости против линейной атаки. Также для оценки стойкости используется таблица линейного распределения или таблица линейной аппроксимации.

Линейный криптоанализ использует преимущества линейных выражений, связывающих между собой биты входных данных, биты выходных данных шифра и биты ключей, которые справедливы с высокой вероятностью.

Пусть $X = [X_1, X_2, ..., X_n]$ и $Y = [Y_1, Y_2, ..., Y_n]$ - n-битные входные и соответствующие выходные данные шифра, где X_i представляет i-й бит входного вектора X, а Y_j представляет j-й бит выходного вектора Y. При линейном криптоанализе шифр аппроксимируется с помощью линейного выражения вида $X_{i_1} \oplus X_{i_2} \oplus ... \oplus X_{i_k} \oplus Y_{j_1} \oplus Y_{j_2} \oplus ... \oplus Y_{j_m} = 0$.

Это уравнение представляет собой сумму по модулю 2 k входных битов и m выходных битов. При проведении линейной атаки злоумышленник определяет подобные линейные выражения, которые имеют высокую или низкую вероятность появления. Нахождение вышеуказанных линейных выражений, выполняемых с большой вероятностью, или невыполняемых с большой вероятностью, показывает слабость шифра. Вероятность выполнения линейного выражения для случайных значений k + m k входных битов и m выходных битов равно 1/2. При линейном криптоанализе используется отклонение или смещение от вероятности выполнения линейного выражения, равной 1/2. Наличие очевидного линейного выражения для всех входных и выходных значений указывает на тривиальную слабость шифра. Линейная атака относится к атакам с использованием открытого текста, при которых предполагается, что злоумышленник имеет информацию о наборе входных данных и соответствующих выходных данных шифра, но не может выбрать, какие входные данные (и соответствующие выходные) доступны.

Оценка иммунитета против линейного криптоанализа является существенной при разработке безопасных блочных шифров. Используя "wide trail design strategy" можно легко посчитать сложность линейной на основе показателя нелинейности S-блока.

Алгебраический криптоанализ. Еще один важный метод криптоанализа – алгебраический криптоанализ. Алгебраическая степень и алгебраическая иммунность являются показателями стойкости против алгебраических атак.

Алгебраический криптоанализ использует внутренние математические структуры, которые имеются в криптографических алгоритмах и пытается определить уязвимости в них. При алгебраическом криптоанализе для описания всего криптографического алгоритма строится алгебраическая система уравнений над конечным [2]. При применении *S*-блоков, обладающих предельно достижимыми показателями свойств, характеризующих степень защиты от статистического криптоанализа, алгебраические системы уравнений, описывающие такие *S*-блоки имеют низкую степень. Нелинейность многих криптоалгоритмов определяется лишь только *S*-блоками, поэтому многие алгоритмы могут быть описаны разреженной алгебраической переопределенной системой всего лишь второй степени [2, 3]. Не существует универсальных методов для решения систем алгебраических нелинейных уравнений над конечными полями. Это в свою очередь обеспечивает практическую криптографическую стойкость алгоритмов.

При алгебраической атаке строится алгебраическая система уравнений над конечным полем низкой степени, которая описывает криптографический алгоритм, и находится её решение.

Основные этапы алгебраического криптоанализа можно описать следующим образом:

1) строится максимальное количество алгебраических уравнений, которые описывают криптографический алгоритм с минимальной степенью составляющих их термов;

2) решается полученная система.

В результате решения находятся биты раундовых ключей.

Чтобы представить криптографический алгоритм шифрования в виде системы уравнений необходимо выполнить следующие действия:

1) Разделить криптографический алгоритм на отдельные составляющие его части, при этом группировать отдельно линейные и нелинейные операции.

2) Построить для каждой структурной части алгоритма систему, которая будет связывать входные и выходные данные этого части алгоритма.

3) Найти связь входных и выходных данных каждой из структурной части алгоритма с другими частями, а также битами ключа, входных и выходных данных всего алгоритма.

После представления отдельных структурнойых частей алгоритма необходимо записать общую систему, описывающую весь алгоритм.

Алгебраическая степень и алгебраический иммунитет являются показателями стойкости против алгебраических атак. Оптимальными значениями алгебраической степени являются значения не меньше 7. Максимальным значением алгебраического иммунитета считается 3 при 441 уравнениях [4].

Существуют также методы, являющимися модификациями и усилениями дифференциального криптоанализа. Они также используют возможные слабости S-блоков, входящих в структуры анализируемых алгоритмов. Это такие методы, как метод бумеранга, метод усеченных дифференциалов, метод невозможных дифференциалов.

Метод бумеранга. В 1999 году профессором университета Беркли (Калифорния, США) Дэвидом Вагнером (David Wagner) было предложено усиление дифференциального криптоанализа, известное под название метода бумеранга (boomerang attack) (см. [5]). Метод бумеранга вместо двух открытых текстов и соответствующих им шифртекстов, связанных определенными соотношениями, как при дифференциальном криптоанализе, использует четверку (квартет) открытых текстов и соответствующих им шифртекстов, связанных определенными соотношениями. Такие соотношения квартетов позволяют успешно производить криптоаналитические атаки на некоторые из криптоалгоритмов, которые в то же время остаются стойкими к обычному дифференциальному криптоанализу. Если же при этом учитывать требуемые объемы данных для атаки, то в некоторых случаях метод бумеранга оказывается более экономичным и эффективным по сравнению с дифференциальным криптоанализом. Атака методом бумеранга также применима к криптографическим алгоритмам с гетерогенной структурой раундов. Метод бумеранга представляет относится к атакам с адаптивным выбором открытых текстов и шифртекстов. Известно, что такие атаки являются наиболее сложно применимыми на практике. Это можно считать своего рода серьезным недостатком метода в сравнении с дифференциальным криптоанализом.

Метод усеченных дифференциалов. Метод усеченных дифференциалов, как и классический метод дифференциального анализа, нацелен на нелинейный узел алгоритма – S-блок.

Метод усеченных дифференциалов является своего рода развитием идеи дифференциального анализа. Метод позволяет рассматривать возможность находить такие характеристики, при которых используются некие так называемые усеченные дифференциалы (truncated differentials). Усеченные дифференциалы представляют собой разности между определенными битами обрабатываемых данных. Вероятности их существенно выше, чем в случае классических «полных» характеристик. Данная атака была разработана Ларсом Кнудсеном в 1994 году [6].

В работе [7] проиллюстрировано свойство блочного симметричного шифра против атаки усеченных дифференциалов в случае наличия хороших перемешивающих блоков шифра. Данное свойство объясняется тем, что при проведении текстов с выбранными характеристиками через раундовые преобразования алгоритма, функция перемешивания алгоритма нарушает все связи между битами указанных характеристик. Другими словами, вероятность прохождения таких характеристик становятся ничтожно малой в силу независимости отдельных раундовых блоков преобразования алгоритма. В работе [8] продемонстрировано, что сложение в конечном поле хорошо перемешивает смежные классы по мультипликативной группе любого подполя и наоборот. Также показано, что операция сложения в конечном поле равномерно перемешивает смежные классы по мультипликативной группе, порядок которой близок к значению квадратного корня из числа элементов в поле. В свою очередь операция умножения в конечном поле сохраняет смежные классы мультипликативной группы по любой мультипликативной подгруппе.

Кроме того, в работах [9, 10] доказана теория об отсутствии эффективных байтовых характеристик для определенного числа раундов для Rijndael-подобных алгоритмов, что свидетельствует о стойкости к атаке усеченных дифференциалов указанного рода алгоритмов.

Метод невозможных дифференциалов. Метод невозможных дифференциалов является еще одним вариантом дифференциального криптоанализа. Этот метод использует так называемые невозможные дифференциалы (impossible differentials), т.е. дифференциалы с нулевой вероятностью. Атака была предложена в 1998 г. в работах [11, 12]. Краткое описание атаки состоит в следующем:

1. Выбираются необходимые пары открытых текстов с требуемой разностью, в результате применения криптоалгоритма получаются соответствующие им шифртексты.

2. Полученные данные анализируются, в результате чего исключаются все варианты ключа шифрования, приводящие к дифференциалам с нулевой вероятностью.

3. После исключения таких ключей остается некое подмножество ключей, которые не приводят к дифференциалам с нулевой вероятностью, и для нахождения верного ключа осуществляется полный перебор этого подмножества.

Существует вариант дифференциального криптоанализа, при котором используются дифференциалы с минимальной вероятностью. При этом действия криптоаналитика аналогичны описанным выше. В работе [13] проиллюстрирован метод доказательства стойкости блочных шифров к атаке невозможных дифференциалов. Также данный метод позволяет обосновать стойкость группы Rijndael-подобных шифров с 4-мя и более циклами к атаке невозможных дифференциалов. В основе вышеуказанного метода для успешного проведения атаки лежит следующая теорема [13].

Теорема. Если для блочного симметричного шифра существует некоторая разность Δ, которая может быть получена из любой ненулевой входной разности за r_1 циклов преобразований и которая может быть получена из любой ненулевой выходной разности за r_2 циклов, выполняемых в направлении дешифрования, то для такого блочного симметричного шифра не существует невозможный дифференциал с r_1+r_2 и более циклами.

Таким образом, для доказательства отсутствия невозможного дифференциала необходимо определить количество циклов r_1 и r_2, за которые любая входная разность и любая выходная могут прийти к некоторому значению разности Δ. С помощью указанной теоремы можно, например, объяснить отсутствие невозможных дифференциалов для многих Rijndael-подобных шифров.

Интегральный криптоанализ. Интегральный криптоанализ рассматривает влияние алгоритма на множество открытых текстов, а не на пару как при дифференциальном криптоанализе. Интегральный криптоанализ объединяет в себе целый ряд криптоаналитических атак криптографические алгоритмы. Интегральный криптоанализ относится к классу атак на раундовую функцию, и для ее реализации необходимо иметь достаточное множество криптограмм, полученных при зашифровании подобранных открытых текстов на одном и том же секретном ключе.

Интегральной атака названа, потому что в атаке рассматривается прохождение через преобразования шифра суммы состояний. Здесь подразличными состояниями понимаются некоторые промежуточные значения блоков преобразуемых данных в процессе их зашифрования. Подобно тому, как в дифференциальном криптоанализе производится “транспортирование” разности через преобразования шифра, в данной атаке через циклы шифра проводится значение суммы состояний из некоторого множества [14].

Если имеется возможность с высокой вероятностью предсказать значение некоторых битов суммы состояний после r циклов шифрования, то это означает, что может быть организована интегральная атака на (r+1)-раундовый шифр. В ходе атаки перебираются возможные подключи последнего раунда и для каждого варианта производится дешифрование одного раунда для всего множества имеющихся криптограмм. Если в результате суммирования информационных блоков, полученных при одноraундовом дешифровании, на известных позициях будет получено нужное значение, то с высокой вероятностью проверяемая часть подключа последнего цикла является верной. Более подробно особенности организации этого вида атак изложены в [15].

3 Заключение

S-блоки являются одним из основных компонентов, определяющих нелинейность и уровень стойкости современных симметричных криптографических алгоритмов. Для защиты алгоритмов от различных видов атак S-блоки должны удовлетворять целому ряду критериев. В настоящее время основными атаками, для которых имеют значения свойства S-блоков, используемых в криптографических алгоритмах, являются атаки, основанные на линейном, дифференциальном, алгебраическом методах криптоанализа.

В работе выполнен обзор существующих методов криптоанализа, использующих возможные слабости в S-блоках.

4 Благодарности

Работа выполнена при финансовой поддержке КН МОН РК, № AP09258274.

Список использованных источников:

1 Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis // Doctoral Dissertation, March 1995, K.U.Leuven. https://cs.ru.nl/~joan/papers/JDA_Thesis_1995.pdf

2 Courtois N.T., Pieprzyk J. Cryptanalysis of block ciphers with over defined systems of equations // Proceedings of Asiacrypt'02, LNCS. Springer-Verlag, Berlin, 2002, pp 267-287. https://doi.org/10.1007/3-540-36178-2_17

3 Олейников Р.В., Казимиров А.В. Построение переопределённой системы уравнений для описания алгоритма шифрования «Лабиринт». // Прикладная радиоэлектроника. Харьков: ХНУРЭ. 2009. Том. 8, № 3. https://openarchive.nure.ua/handle/document/726

4 Казимиров А.В. Методы и средства генерации нелинейных узлов замены для симметричных криптоалгоритмов. Диссертация на соискание учёной степени кандидата технических наук, специальность 05.13.21 – системы защиты информации. Харьковский национальный университет радиоэлектроники, Харьков, 2013.

5 David Wagner (March 1999). "The Boomerang Attack"6th International Workshop on Fast Software Encryption (FSE '99). Rome: Springer-Verlag. pp.156–170, FIPS-197: Advanced Encryption Standard, November 2001. pp 156-170. https://doi.org/10.1007/3-540-48519-8_12

6 Knudsen L. Truncated and higher order differentials. Proceedings of the Second international workshop Fast Software Encryption, LNCS 1008, Springer-Verlag, 1995, P. 196-211. DOI: 10.1007/3-540-60590-8_16

7 Standaert F.-X., Piret G., Quisquater J.-J. Cryptanalysis of Block Ciphers: A Survey. http://citeseer.ist.psu.edu – Universite catolique de Louvain, Belgium, 2003. https://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/U1.pdf

8 Шемякина О.В. О перемешивающих свойствах операций в конечном поле, Дискретная математика, т. 23:2, 2011, С. 32-40. DOI: https://doi.org/10.4213/dm1138

9 Руженцев В.И. Доказуемая стойкость Rijndael-подобных шифров к атаке усеченных дифференциалов, Радіоелектронні і комп'ютерні системи, 2012, № 5, С. 51–55. http://nbuv.gov.ua/UJRN/recs_2012_5_11

10 Руженцев В.И. О стойкости к атаке усеченных дифференциалов Rijndael-подобных шифров с большими размерами блоков, ВІСНИК НУК, 2013.

11 Biham E., Biryukov A., Shamir A. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials, Proceeding of EUROCRYPT '99, LNCS 1592, Springer-Verlag, 1999, P.12–23. https://doi.org/10.1007/3-540-48910-X_2

12 Biham E., Biryukov A., Shamir A. Miss in the Middle Attacks on IDEA and Khufu, Proceedings of the Sixth international workshop Fast Software Encryption, LNCS 1636, Springer-Verlag, 1999, P. 124-138. https://link.springer.com/content/pdf/10.1007%2F3-540-48519-8_10.pdf

13 Руженцев В.И. О методе доказательства стойкости блочных шифров к атаке невыполнимых дифференциалов, Прикладная радиоэлектроника, том 12, № 2, 2013, С. 215-219. http://nbuv.gov.ua/UJRN/Prre_2013_12_2_8

14 В.И. Руженцев, О стойкости блочных шифров с Rijndael-подобными преобразованиями к интегральным атакам,Прикладная радиоэлектроника, 2012, Том 11, № 2, стр. 160-164.

15 Knudsen L. R. Integral Cryptanalysis, NESSIE internal report NES/DOC/UIB/WP5/015/1, 2001. https://doi.org/10.1007/3-540-45661-9_9

References:

1 Daemen J. Cipher and hash function design strategies based on linear and differential cryptanalysis // Doctoral Dissertation, March 1995, K.U.Leuven. https://cs.ru.nl/~joan/papers/JDA_Thesis_1995.pdf

2 Courtois N.T., Pieprzyk J. Cryptanalysis of block ciphers with over defined systems of equations // Proceedings of Asiacrypt'02, LNCS. Springer-Verlag, Berlin, 2002, pp 267-287. https://doi.org/10.1007/3-540-36178-2_17

3 Olejnikov R.V., Kazimirov A.V. (2009) Postroenie pereopredeljonnoj sistemy uravnenij dlja opisanija algoritma shifrovanija «Labirint»[Oleinikov R.V., Kazimirov A.V. Construction of an overdetermined system of equations to describe the encryption algorithm "Labyrinth"]. Applied Radio Electronics. Kharkiv: KhNURE. Vol. 8, No. 3. (In Russian) https://openarchive.nure.ua/handle/document/726

4 Kazimirov A.V. (2013) Metody i sredstva generacii nelinejnyh uzlov zameny dlja simmetrichnyh kriptoalgoritmov [Methods and tools for generating nonlinear substitution nodes for symmetric cryptoalgorithms]. Dissertation for the degree of candidate of technical sciences, specialty 05.13.21 - information security systems. Kharkiv National University of Radio Electronics, Kharkiv, (In Russian)

5 David Wagner (March 1999). "The Boomerang Attack"6th International Workshop on Fast Software Encryption (FSE '99). Rome: Springer-Verlag. pp.156–170, FIPS-197: Advanced Encryption Standard, November 2001. pp 156-170. https://doi.org/10.1007/3-540-48519-8_12

6 Knudsen L. Truncated and higher order differentials. Proceedings of the Second international workshop Fast Software Encryption, LNCS 1008, Springer-Verlag, 1995, P. 196-211. DOI: 10.1007/3-540-60590-8_16

7 Standaert F.-X., Piret G., Quisquater J.-J. Cryptanalysis of Block Ciphers: A Survey. http://citeseer.ist.psu.edu – Universite catolique de Louvain, Belgium, 2003. https://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/U1.pdf

8 Shemjakina O.V. (2011) O peremeshivajushhih svojstvah operacij v konechnom pole [On the mixing properties of operations in a finite field]. Discrete Mathematics, vol. 23: 2, 32-40. DOI: https://doi.org/10.4213/dm1138 (In Russian)

9 Ruzhencev V.I. (2012) Dokazuemaja stojkost' Rijndael-podobnyh shifrov k atake usechennyh differencialov [Proven resistance of Rijndael-like ciphers to attack of truncated differentials]. Radioelectronic and computer systems, No 5, 51–55. http://nbuv.gov.ua/UJRN/recs_2012_5_11 (In Russian)

10 Ruzhencev V.I. (2013) O stojkosti k atake usechennyh differencialov Rijndael-podobnyh shifrov s bol'shimi razmerami blokov [On the resistance to attack of truncated differentials of Rijndael-like ciphers with large block sizes], VISNIK NUK, (In Russian)

11 Biham E., Biryukov A., Shamir A. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials, Proceeding of EUROCRYPT '99, LNCS 1592, Springer-Verlag, 1999, P.12–23. https://doi.org/10.1007/3-540-48910-X_2

12 Biham E., Biryukov A., Shamir A. Miss in the Middle Attacks on IDEA and Khufu, Proceedings of the Sixth international workshop Fast Software Encryption, LNCS 1636, Springer-Verlag, 1999, P. 124-138. https://link.springer.com/content/pdf/10.1007%2F3-540-48519-8_10.pdf

13 Ruzhencev V.I. (2013) O metode dokazatel'stva stojkosti blochnyh shifrov k atake nevypolnimyh differencialov [On the method of proving the resistance of block ciphers to the attack of impracticable differentials]. Applied Radio Electronics, vol. 12, no. 2, 215-219. http://nbuv.gov.ua/UJRN/Prre_2013_12_2_8 (In Russian)

14 V.I. Ruzhencev (2012) O stojkosti blochnyh shifrov s Rijndael-podobnymi preobrazovanijami k integral'nym atakam [On the resistance of block ciphers with Rijndael-like transformations to integral attacks]. Applied Radioelectronics, Volume 11, No. 2, 160-164. (In Russian)

15 Knudsen L. R. Integral Cryptanalysis, NESSIE internal report NES/DOC/UIB/WP5/015/1, 2001. https://doi.org/10.1007/3-540-45661-9_9.