А. А. Перов, А. И. Пестунов, О возможности применения свёрточных нейронных сетей к построению универсальных атак на итеративные блочные шифры, *ПДМ*, 2020, номер 49, 46–56

DOI: https://doi.org/10.17223/20710410/49/4

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.7

О ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ СВЁРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ К ПОСТРОЕНИЮ УНИВЕРСАЛЬНЫХ АТАК НА ИТЕРАТИВНЫЕ БЛОЧНЫЕ ШИФРЫ

А. А. Перов*, А. И. Пестунов**

**Московский политехнический университет, г. Москва, Россия*

***Новосибирский государственный университет экономики и управления "НИНХ", г. Новосибирск, Россия*

Исследуется возможность применения свёрточных нейронных сетей к задаче анализа стойкости итеративных блочных шифров. Предлагается новый подход к построению атак-различителей на основе свёрточной нейронной сети, обученной различать графические эквиваленты шифртекстов, полученных в режиме шифрования CTR (счётчика) после разного числа раундов, в том числе после такого, которое обеспечивает удовлетворительные статистические свойства шифртекста. По аналогии со статистическими тестами, предложенный подход позволяет создавать различители без необходимости проведения аналитического исследования каждого шифра, что даёт возможность строить универсальные различители сразу для серии шифров. Предлагается несколько схем построения универсальных атак-различителей, которые, как демонстрируется экспериментально, в ряде случаев позволяют выявлять отклонения от случайности на меньших выборках и при большем числе раундов, чем ранее известные статистические тесты.

Ключевые слова: *блочный шифр, машинное обучение, нейронная сеть, статистический анализ, атака-различитель, криптоанализ.*

DOI 10.17223/20710410/49/4

ON POSSIBILITY OF USING CONVOLUTIONAL NEURAL NETWORKS FOR CREATING UNIVERSAL ATTACKS ON ITERATIVE BLOCK CIPHERS

A. A. Perov*, A. I. Pestunov**

**Moscow Polytechnic University, Moscow, Russia*

***Novosibirsk State University of Economics and Management, Novosibirsk, Russia*

E-mail: perov_artem@inbox.ru, pestunov@gmail.com

The paper explores possibility of applying convolutional neural networks to the security analysis of iterative block ciphers. A new approach for constructing distinguishing attacks based on a convolutional neural network is proposed. The approach is based on distinguishing between graphic equivalents of ciphertexts received by the CTR (counter) encryption mode after different number of rounds, including the number of rounds guaranteeing satisfaction of statistical properties. Several schemes are presented for constructing distinguishing attacks, which in some cases make it possible

to detect deviations from randomness in smaller samples than previously known, and with a large number of rounds. The approach allows to create distinguishers without the need for an analytical research of each cipher, which makes it possible to build universal distinguishers for a series of ciphers.

Keywords: *block cipher, machine learning, neural network, statistical analysis, distinguishing attack, cryptanalysis.*

Введение

Итеративные блочные шифры позволяют решать обширный круг задач и являются одним из наиболее значимых и часто используемых классов криптографических алгоритмов. Такие шифры состоят из раундов шифрования — простых итераций, достаточное количество которых обеспечивает требуемый уровень стойкости. Итеративная структура блочных шифров обуславливает выбор подходов к их криптоанализу. Одной из часто применяемых атак является атака-различитель (англ. disinguishing attack), предназначенная для распознавания шифртекстов, полученных после разного числа раундов. При этом важной задачей является поиск максимального числа раундов, при котором возможно построить такую атаку, и уменьшение размера выборки, при котором удаётся обнаружить отклонения от случайности. Эффективные различители представляют интерес как сами по себе, так и в комплексе, когда на их основе создаются алгоритмы вычисления секретных ключей шифрования.

Методы построения атак-различителей можно условно разделить на два класса: аналитические и эмпирические (в основном статистические). Многие аналитические методы базируются на выявлении дифференциальных [1 – 3], линейных [4] или интегральных [5, 6] признаков, описывающих определённые свойства шифртекста после заданного числа раундов (r) и называемых r-раундовыми характеристиками. На основании этих характеристик разрабатываются алгоритмы вычисления ключа, используемого на $(r + 1)$-м и последующих раундах посредством их полного или частичного перебора. Роль характеристик в этом процессе состоит в том, чтобы отбрасывать неверные пробные ключи (при расшифровании одного $(r+1)$-го раунда с верным ключом r-раундовая характеристика выполняется, а при неверном — нет).

Аналитические различители характерны тем, что они позволяют строить атаки на большое количество раундов, когда требуются огромные вычислительные ресурсы, недоступные на практике (например, порядка 2^{128} элементарных операций или бит оперативной памяти). Однако поскольку признаки, используемые в таких различителях, обычно тесно связаны с конкретными шифрами, то они не являются универсальными и эффективны только для ограниченного набора шифров. Имеются работы, в которых атаки на блочные шифры и их свойства описываются в общем виде, но, как правило, делается это на довольно высоком уровне абстракции, что не позволяет применить их к серии шифров без дополнительного анализа [7, 8]. При этом, если структура шифра хотя бы частично конкретизирована и позволяет описать класс шифров, то аналитические оценки и атаки можно распространять на такие классы [9 – 11].

Помимо аналитических методов, для оценки стойкости итеративных блочных шифров могут использоваться эмпирические статистические методы, позволяющие осуществить атаку-различитель в ходе эксперимента на выборке, размер которой приемлем для расчётов [12, 13]. Так, в работе [14] предложен и применён для шифра RC6 универсальный подход к вычислению ключа шифрования, где в качестве атаки-различителя выступает критерий хи-квадрат. Для малого числа раундов, когда для распознавания

отклонения от случайности достаточно небольших выборок, атака осуществляется экспериментально, а для большего числа раундов размер выборки экстраполируется аналитически на основе экспериментальных данных. В рамках этого подхода предложены и успешно применены атаки на основе статистических тестов, использующих динамически изменяемые структуры [15 – 17], что позволило повысить их эффективность для ряда шифров [18 – 20].

Достоинством статистических методов является их универсальность, поскольку по одной и той же схеме можно проанализировать серию шифров без учёта особенностей каждого из них. При этом необходимость проведения экспериментальных расчётов накладывает ограничения на размер выборки. Использование свёрточных нейронных сетей имеет потенциал для снижения размера выборки за счёт учёта паттернов, встречающихся в шифртекстах, в то время как статистические тесты принимают решение на основе неких интегральных характеристик, которые хотя и обновляются после каждого выборочного значения, но не рассматривают всю выборку целиком. Технологии машинного обучения уже применяются в криптоанализе, но в основном они связаны с атаками по побочным каналам [21, 22]. Кроме того, многие эффективные атаки в стегоанализе также используют технологии машинного обучения, в том числе ансамблевые классификаторы и метод опорных векторов [24 – 26].

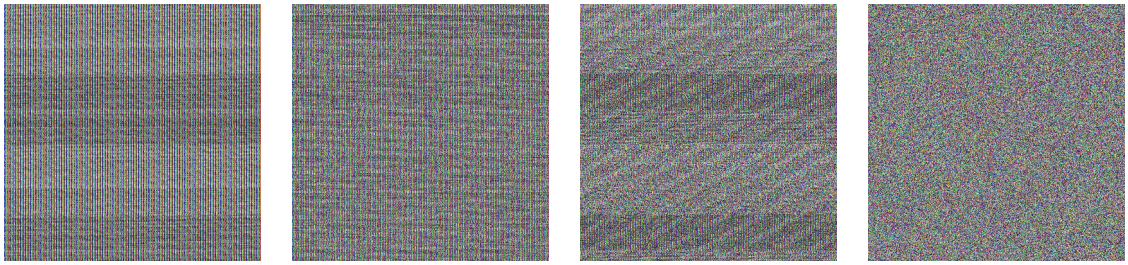
В настоящей работе показано, что свёрточные нейронные сети могут быть использованы для построения универсальных атак-различителей, которые, как демонстрируется экспериментально, в некоторых случаях позволяют выявлять отклонения от случайности на меньших выборках и при большем числе раундов, чем ранее известные статистические тесты.

1. Постановка задачи и идея предлагаемого подхода

Задача статистического анализа итеративных блочных шифров состоит в том, чтобы построить атаку-различитель, способную распознать шифртекст после заданного числа раундов, т. е. отличить его от случайной последовательности либо от шифртекста при другом числе раундов. Статистические тесты решают эту задачу посредством вычисления неких интегральных характеристик, которые затем сравниваются с табличными критическими значениями [15 – 17]. При превышении такого значения последовательность признаётся неслучайной с вероятностью $1 - \alpha$, где α — заданный уровень значимости (допустимая вероятность ошибки статистического теста при проверке истинно случайной последовательности). Как правило, с увеличением числа раундов шифрования растёт размер выборки, на котором тест способен отличить шифртекст от случайной последовательности, поэтому этот размер используется для определения числа раундов [12 – 14, 19, 20].

Идея предлагаемого подхода возникла в результате наблюдения, что преобразованный в растровое изображение шифртекст итеративного блочного шифра при разном числе раундов имеет выраженную текстуру (паттерн), которая с увеличением числа раундов изменяется в сторону равномерно шумного (случайного) изображения. Например, на рис. 1 представлены графические эквиваленты шифртекстов итеративного блочного шифра Simon с размером блока 32 бита (Simon-32) после 3, 6, 9 и 30 раундов шифрования.

Рабочая гипотеза нашего исследования заключается в том, что нейронная сеть, решающая задачи классификации изображений, способна различать и шифртексты, полученные при разном числе раундов.



3 раунда 6 раундов 9 раундов 30 раундов

Рис. 1. Различие текстур в графических эквивалентах шифртекстов блочного шифра Simon-32 после разного числа раундов

1.1. Инструментарий для проведения экспериментов

Экспериментальное исследование проводилось с помощью нейронной сети Inception-v3 [23], показавшей высокие результаты по распознаванию изображений на конкурсе ImageNet-2014, а предложенная позднее модификация позволила ещё больше увеличить её эффективность.

На основании предварительного анализа для обеспечения приемлемого баланса между скоростью обучения нейронной сети и точностью классификации выбраны следующие параметры: размер изображения составляет 400×400 цветных RGB-пикселей, а размер партии равен 32.

Шифртексты преобразуются в цветные изображения посредством специально разработанной утилиты на языке C++, которая считывает файл с шифртекстом в бинарном виде и записывает каждый байт в качестве значения компонент палитры RGB, формируя 24-битовое растровое BMP-изображение. База шифртекстов для экспериментов формируется с помощью программной библиотеки [27], предназначенной для удобного шифрования сообщений при разном числе раундов.

Размер изображения 400×400 пикселей соответствует выборке размера приблизительно $2^{21{,}9}$ бит: каждый из 160000 пикселей кодируется 24 битами (по 1 байту на каждую компоненту палитры RGB).

Эффективность различителей (способность нейронной сети отличать шифртексты при различном числе раундов друг от друга и от случайных последовательностей) оценивается через долю верных решений нейронной сети на элементах контрольной выборки следующим образом. Пусть n — размер контрольной выборки. Введём следующие случайные величины для $i = 1, \ldots, n$:

$$\eta_i = \begin{cases} 1, \text{если нейронная сеть приняла верное решение} \\ \qquad \text{на } i\text{-м изображении из контрольной выборки}, \\ 0 \quad \text{иначе.} \end{cases}$$

Тогда количество верных решений нейронной сети (S_n) и их долю ($\tilde{S}_n$) на всей контрольной выборке можно определить следующим образом:

$$S_n = \sum_{i=1}^{n} \eta_i, \quad \tilde{S}_n = S_n / n.$$

Найдём такое $\tilde{\delta}(n, \alpha)$, что при $\tilde{S}_n \notin [1/2 - \tilde{\delta}(n, \alpha), 1/2 + \tilde{\delta}(n, \alpha)]$ можно сделать вывод о том, что нейронная сеть способна отличать шифртексты и случайные последовательности друг от друга эффективнее простого угадывания.

Пусть

$$S_n^* = \frac{S_n - \mathbb{E}S_n}{\sqrt{\mathbb{D}S_n}}, \tag{1}$$

где $\mathbb{E}S_n$ и $\mathbb{D}S_n$ — математическое ожидание и дисперсия S_n соответственно. Из центральной предельной теоремы следует, что

$$\mathsf{P}\left[S_n^* \in [-\delta, \delta]\right] \approx F_{0,1}(\delta) - F_{0,1}(-\delta),$$

где $F_{0,1}(\cdot)$ — функция стандартного нормального (гауссовского) распределения.

Пусть $Q_{\alpha/2} = F_{0,1}^{-1}(1 - \alpha/2)$ — квантиль стандартного нормального распределения уровня $1 - \alpha/2$, тогда

$$\mathsf{P}\left[S_n^* \in [-Q_{\alpha/2}, Q_{\alpha/2}]\right] \approx 1 - \alpha. \tag{2}$$

Если нейронная сеть не способна отличать графические эквиваленты шифртекстов или случайных последовательностей друг от друга, то все случайные величины η_i имеют распределение Бернулли с параметром 1/2, т. е. $\mathsf{P}[\eta_i = 1] = \mathsf{P}[\eta_i = 0] = 1/2$, поскольку результат работы нейронной сети равносилен случайному угадыванию. Следовательно, $\mathbb{E}S_n = n/2$ и $\mathbb{D}S_n = n/4$, а формулу (1) можно преобразовать к виду

$$S_n^* = \frac{S_n - n/2}{\sqrt{n}/2} = \frac{2S_n - n}{\sqrt{n}}. \tag{3}$$

Из формул (2) и (3) получаем

$$\tilde{\delta}(\alpha, n) = \frac{Q_{\alpha/2}}{2\sqrt{n}}. \tag{4}$$

Например, при $\alpha = 0{,}01$ величина $Q_{0{,}01/2}$ равна 2,59, и при таких значениях $\tilde{\delta}(0{,}01, 200) = 0{,}09$ и $\tilde{\delta}(0{,}01, 2000) = 0{,}03$.

2. Экспериментальные результаты

Далее представлены результаты экспериментов по различению итеративных блочных шифров при варьируемом числе раундов и случайных последовательностей. Предложено четыре схемы экспериментов, набор которых может быть расширен и другими вариантами.

2.1. Базовая схема 1: различение случайной последовательности и шифртекста при сокращённом числе раундов

Задачей первой схемы экспериментов является выявление принципиальной способности нейронной сети отличать случайные последовательности от шифртекста при сокращённом числе раундов. В качестве случайной последовательности взят шифртекст, полученный с помощью 14-раундового шифра AES в режиме счётчика, поскольку многочисленные исследования до настоящего времени не выявили у этого шифра каких-либо уязвимостей, значимых с практической точки зрения. Например, в работе [13] показано, что уже начиная с трёх раундов шифртекст AES обладает удовлетворительными статистическими свойствами. В качестве исследуемого шифра взят шифр Simon-32, поскольку, согласно предварительным экспериментам, статистические свойства его шифртекста достаточно равномерно (без скачков) улучшаются с увеличением числа раундов, что даёт возможность наглядно представить результаты, касающиеся способности нейронной сети находить отклонения от случайности.

Для проведения экспериментов сгенерированы по 1000 шифртекстов алгоритма Simon-32 с различным числом раундов и 1000 случайных последовательностей с помощью 14-раундового AES. Затем для каждого эксперимента нейронная сеть обучалась с целью различения r-раундового Simon-32 и случайных последовательностей, $r = 1, \ldots, 10$.

Результаты экспериментов приведены в табл. 1, которая демонстрирует, что при малом числе раундов нейронная сеть приняла 100 % верных решений, а с ростом их числа процент ошибок увеличивается. Тем не менее до 15-го раунда процент ошибок существенно меньше 50 %, т. е. вероятности произвольного угадывания.

Таблица 1

Оценка способности нейронной сети отличать случайные последовательности от шифртекста при сокращённом числе раундов

Число раундов	3	5	7	9	11	13	15	17	19	21
Доля верных решений	1,00	1,00	1,00	0,98	0,91	0,70	0,52	0,53	0,49	0,50

Поскольку в экспериментах по данной схеме размер контрольной выборки $n = 400$, то при $\alpha = 0{,}01$ по формуле (4) получаем $\tilde{\delta}(0{,}01, 400) \approx 0{,}065$, следовательно, если доля верных решений лежит за пределами интервала [0,43; 0,57], то с вероятностью 0,99 можно считать, что r-раундовый шифртекст отличим от случайной последовательности. Таким образом, из результатов табл. 1 можно сделать вывод о том, что при $r \leqslant 15$ блочный шифр Simon не обладает удовлетворительными статистическими свойствами, а при большем числе раундов нейронная сеть способна принимать только решение, равносильное угадыванию.

В работе [12] представлены атаки-различители для шифра Simon-32 (с разными размерами блока) на основе статистического теста «стопка книг» [17]. Максимальное число раундов, при котором выявлены отклонения от случайности у этого шифра, равно 12 на выборке размера 2^{36} бит. Этот результат достигнут для 64-битового блока. Для Simon с 32-битовым блоком отклонения от случайности найдены для 9 раундов на выборке размера 2^{27}. Таким образом, можно сделать вывод, что нейронная сеть способна отличить от случайности большее число раундов и на меньших выборках.

2.2. Схема 2: различение соседних раундов

Следующая схема может применяться, например, в отсутствие источника случайных чисел. Она сравнивает графические эквиваленты шифртекстов соседних раундов итеративного блочного шифра. В качестве обучающей выборки на вход подаются зашифрованные алгоритмом Simon-32 последовательности с 3 по 21 раунд (по 400 изображений на каждый). Задача состоит в том, чтобы выяснить, насколько нейронная сеть способна отличать соседние раунды друг от друга.

На рис. 2 представлены результаты экспериментов. Обратим внимание, что линия тренда постепенно сходится к 0,5, т. е. нейронной сети становится сложнее распознавать шифртексты. Найдём число раундов, при котором нейронная сеть способна отличать шифртексты от случайной последовательности в рамках данной схемы. Здесь размер контрольной выборки $n = 200$, значит, $\tilde{\delta}(0{,}01, 200) \approx 0{,}092$, следовательно, если нейронная сеть способна выявлять отклонения, то доля верных решений должна лежать за пределами интервала [0,408; 0,592]. Таким образом, заключаем, что при $r \leqslant 14$ блочный шифр Simon не обладает удовлетворительными статистическими свойствами, а при большем числе раундов нейронная сеть способна только угадывать. Видно, что в рамках данной схемы нейронная сеть работает менее эффективно, чем в рамках

базовой схемы (отличает на 1 раунд меньше), но по-прежнему эффективнее атаки-различителя из работы [12].

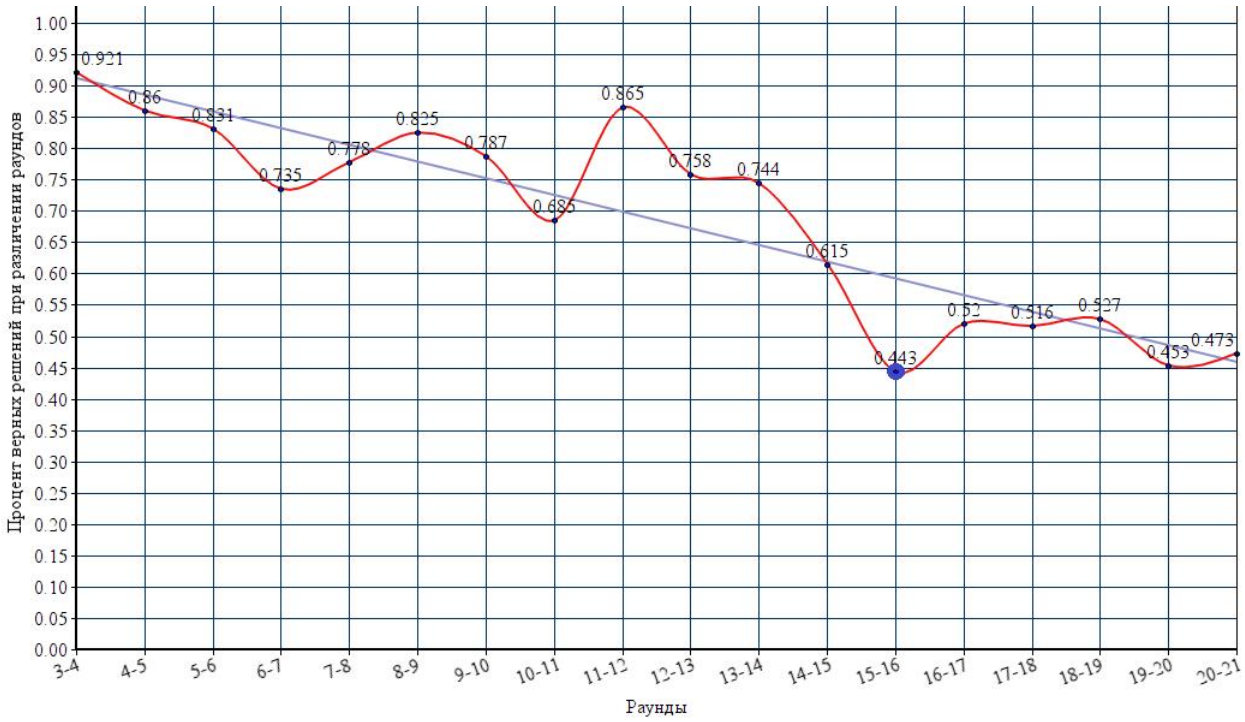


Рис. 2. Оценка способности нейронной сети различать соседние раунды шифра

2.3. Схема 3: различение двух шифров

Цель данной схемы — проанализировать, насколько нейронная сеть способна отличать шифры друг от друга. Для экспериментов выбраны блочные шифры Speck-32 и Present, поскольку, согласно предварительному анализу, они демонстрируют похожие статистические свойства при одинаковом числе раундов (наиболее сложный для нейронной сети случай).

Для каждого из анализируемых раундов формируется обучающая выборка размера 800 (включающая по 400 графических эквивалентов шифртекстов каждого из двух шифров при равном числе раундов). Контрольная выборка имеет размер 200 и включает по 100 шифртекстов каждого шифра. Результаты представлены в табл. 2. Как и в схеме 2, здесь $n = 200$, $\tilde{\delta}(0{,}01, 200) = 0{,}092$ и интервал для доли верных решений — [0,408; 0,592].

Таблица 2

Оценка способности нейронной сети различать шифртексты разных шифров при варьируемом числе раундов

Число раундов	3	4	5	6	7	8	9	10
Доля верных решений	1,00	1,00	0,99	1,00	0,91	0,66	0,59	0,49

Таким образом, делаем вывод, что нейронная сеть способна различать эти шифры до 10 раундов. Эти результаты напрямую нельзя сравнивать с результатами [12] (решаются разные задачи), где построена атака-различитель для 6 раундов, однако в целом они согласуются. Кроме того, результаты согласуются и с работой [27], где представлен различитель для 8 раундов шифра Present.

2.4. Схема 4: различение случаев $r < R_{\min}$ и $r \geqslant R_{\min}$ для нескольких шифров

Данная схема предназначена для того, чтобы выяснить, насколько нейронная сеть способна отличать случайные последовательности от шифртекстов, полученных с помощью различных шифров вперемешку при числе раундов, меньшем, чем найденные в работе [27] значения $R_{\min}$.

Обучающая выборка сформирована из графических эквивалентов 8500 шифртекстов, полученных с помощью 16 шифров (по 500 шифртекстов для каждого) и 500 шифртекстов, полученных с помощью 14-раундового AES, которые считаем случайными последовательностями. Проанализированы шифры LBlock, Present, XTEA, Twine, Speck, Clefia, Hight, Piccolo, Klein, Skipjack, mCrypton, LED, Noekeon, Sea, Mibs, DESXL. Контрольная выборка имеет размер 2000 и составлена из 1000 шифртекстов и 1000 случайных последовательностей.

По результатам экспериментов нейронная сеть приняла верное решение на 0,98 доли выборок. В данном случае $n = 2000$, $\tilde{\delta}(0{,}01, 2000) = 0{,}029$ и интервал — $[0{,}471; 0{,}529]$. Таким образом, доля верных решений лежит за пределами этого интервала и можно сделать вывод о способности нейронной сети находить отклонения от случайности по этой схеме.

Заключение

Сформулируем основные выводы по итогам экспериментов.

1) Нейронная сеть способна различать шифртексты одного и того же итеративного блочного шифра при полном и сокращённом числе раундов.
2) Нейронная сеть способна различать шифртексты, полученные при шифровании соседними раундами одного блочного шифра.
3) Нейронная сеть способна различать шифртексты, полученные при помощи разных шифров.
4) Нейронная сеть способна отличать шифртексты, полученные при $r < R_{\min}$, от шифртекстов, полученных при $r \geqslant R_{\min}$, в том числе для разных шифров.
5) На примере блочного шифра Simon-32 показано, что для некоторых шифров различители на основе нейронных сетей могут быть эффективнее: требовать меньшую выборку либо работать на большем числе раундов.

В дальнейшем с помощью предложенного подхода можно вычислять $R_{\min}$ и строить алгоритмы вычисления секретного ключа, используя различители на основе нейронных сетей.

ЛИТЕРАТУРА

1. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. V. 4. P. 3–72.
2. *Knudsen L.* Truncated and higher order differentials // LNCS. 1994. V. 1008. P. 196–211.
3. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials // J. Cryptology. 2005. V. 18. P. 291–311.
4. *Matsui M.* Linear cryptanalysis method for DES cipher // LNCS. 1994. V. 765. P. 386–397.
5. *Knudsen L.* Integral cryptanalysis // LNCS. 2002. V. 2365. P. 112–127.
6. *Biryukov A. and Shamir A.* Structural cryptanalysis of SASAS // J. Cryptology. 2010. V. 23. P. 505–518.

7. *Агибалов Г. П.* Элементы теории дифференциального криптоанализа итеративных блочных шифров с адаптивным раундовым ключом // Прикладная дискретная математика. 2008. № 1(1). С. 34–42.
8. *Денисов О. В.* Критерии марковости алгоритмов блочного шифрования // Прикладная дискретная математика. 2018. № 41. С. 28–37.
9. *Денисов О. В., Былина Р. А.* Матричная формула для распределения выхода блочной схемы шифрования и статистический критерий на ее основе // Прикладная дискретная математика. 2016. № 2(32). С. 33–48.
10. *Токарева Н. Н.* О квадратичных аппроксимациях в блочных шифрах // Проблемы передачи информации. 2008. № 3. С. 105–127.
11. *Агибалов Г. П.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
12. *Сосков А. С., Рябко Б. Я.* Применение атаки различения на легковесные блочные шифры, основанные на ARX-операциях // Вычислительные технологии. 2019. Т. 24. № 3. С. 106–116.
13. *Пестунов А. И.* Статистический анализ современных блочных шифров // Вычислительные технологии. 2007. Т. 12. № 2. С. 122–129.
14. *Knudsen L. and Meier W.* Correlations in RC6 with a reduced number of rounds // LNCS. 2001. V. 1978. P. 94–108.
15. *Рябко Б. Я., Стогниенко В. С., Шокин Ю. И.* Адаптивный критерий хи-квадрат для различения близких гипотез при большом числе классов и его применение к некоторым задачам криптографии // Проблемы передачи информации. 2003. Т. 39. № 2. С. 53–62.
16. *Монарев В. А., Рябко Б. Я.* Экспериментальный анализ генераторов псевдослучайных чисел при помощи нового статистического теста // Журнал вычисл. матем. и матем. физики. 2004. Т. 44. № 5. С. 766–770.
17. *Рябко Б. Я., Пестунов А. И.* «Стопка книг» как новый статистический тест для случайных чисел // Проблемы передачи информации. 2004. Т. 40. № 1. С. 73–78.
18. *Рябко Б. Я., Монарев В. А., Шокин Ю. И.* Новый тип атак на блоковые шифры // Проблемы передачи информации. 2005. Т. 41. № 4. С. 97–107.
19. *Монарев В. А.* Реализация новой статистической атаки на блочный шифр // Вестник СибГУТИ. 2014. № 1. С. 85–90.
20. *Лысяк А. С., Рябко Б. Я., Фионов А. Н.* Анализ эффективности градиентной статистической атаки на блоковые шифры RC6, MARS, CAST-128, IDEA, Blowfish в системах защиты информации // Вестник СибГУТИ. 2013. № 1. С. 85–109.
21. *Lerman L., Bontempi G., and Markowitch O.* A machine learning approach against a masked AES // J. Cryptogr. Eng. 2015. V. 5. P. 123–139.
22. *Hettwer B., Gehrer S., and Guneysu T.* Applications of machine learning techniques in side-channel attacks: a survey // J. Cryptogr. Eng. 2020. V. 10. P. 135–162.
23. *Szegedy C., Vanhoucke V., Ioffe S., et al.* Rethinking the inception architecture for computer vision // Proc. IEEE Conf. CVPR. Las Vegas, NV, USA, June 27–30, 2016. P. 2818–2826.
24. *Монарев В. А., Пестунов А. И.* Эффективное обнаружение стеганографически скрытой информации посредством интегрального классификатора на основе сжатия данных // Прикладная дискретная математика. 2018. № 40. С. 59–71.
25. *Монарев В. А., Пестунов А. И.* Повышение эффективности методов стегоанализа при помощи предварительной фильтрации контейнеров // Прикладная дискретная математика. 2016. №. 2(32). С. 87–99.
26. *Kodovsky J., Fridrich J., and Holub V.* Ensemble classifiers for steganalysis of digital media // IEEE Trans. Inform. Forensics and Security. 2010. V. 7. No. 2. P. 434–444.

27. *Пестунов А. И., Перов А. А.* Программная библиотека для статистического анализа итеративных блочных шифров // Информационное противодействие угрозам терроризма. 2015. № 24. С. 197–202.

REFERENCES

1. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems. J. Cryptology, 1991, vol. 4, pp. 3–72.
2. *Knudsen L.* Truncated and higher order differentials. LNCS, 1994, vol. 1008, pp. 196–211.
3. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. J. Cryptology, 2005, vol. 18, pp. 291–311.
4. *Matsui M.* Linear cryptanalysis method for DES cipher. LNCS, 1994, vol. 765, pp. 386–397.
5. *Knudsen L.* Integral cryptanalysis. LNCS, 2002, vol. 2365, pp. 112–127.
6. *Biryukov A. and Shamir A.* Structural cryptanalysis of SASAS. J. Cryptology, 2010, vol. 23, pp. 505–518.
7. *Agibalov G. P.* Elementy teorii differencial'nogo kriptoanaliza iterativnyh blochnyh shifrov s adaptivnym raundovym klyuchom [Some theoretical aspects of differential cryptanalysis of the iterated block ciphers with additive round key]. Prikladnaya Diskretnaya Matematika, 2008, no. 1(1), pp. 34–42. (in Russian)
8. *Denisov O. V.* Kriterii markovosti algoritmov blochnogo shifrovaniya [Markov criteria for block cipher algorithms]. Prikladnaya Diskretnaya Matematika, 2018, no. 41, pp. 28–37. (in Russian)
9. *Denisov O. V. and Bylina R. A.* Matrichnaya formula dlya raspredeleniya vyhoda blochnoj skhemy shifrovaniya i statisticheskij kriterij na ee osnove [Matrix formula for the spectrum of output distribution of block cipher scheme and statistical criterion based on this formula]. Prikladnaya Diskretnaya Matematika, 2016, no. 2(32), pp. 33–48. (in Russian)
10. *Tokareva N. N.* O kvadratichnyh approksimaciyah v blochnyh shifrah [About quadratic approximations in block ciphers]. Problemy Peredachi Informacii, 2008, vol. 3, pp. 105–127. (in Russian)
11. *Agibalov G. P.* Substitution block ciphers with functional keys. Prikladnaya Diskretnaya Matematika, 2017, no. 38, pp. 57–65.
12. *Soskov A. S. and Ryabko B. Ya.* Primenenie ataki razlicheniya na legkovesnye blochnye shifry, osnovannye na ARX-operaciyah [Applying distinction attack on lightweight block ciphers based on ARX operations] Vychislitel'nye Tekhnologii, 2019, vol. 3, pp. 106–116. (in Russian)
13. *Pestunov A. I.* Statisticheskij analiz sovremennyh blochnyh shifrov [Statistical analysis of modern block ciphers]. Vychislitel'nye Tekhnologii, 2007, vol. 12, no. 2, pp. 122–129. (in Russian)
14. *Knudsen L. and Meier W.* Correlations in RC6 with a reduced number of rounds. LNCS, 2001, vol. 1978, pp. 94–108.
15. *Ryabko B. Ya., Stognienko V. S., and SHokin Yu. I.* Adaptivnyj kriterij hi-kvadrat dlya razlicheniya blizkih gipotez pri bol'shom chisle klassov i ego primenenie k nekotorym zadacham kriptografii [Adaptive Chi-square test for distinguishing close hypotheses with a large number of classes and its application to some cryptography problems]. Problemy Peredachi Informacii, 2003, vol. 39, no. 2, pp. 53–62. (in Russian)
16. *Monarev V. A. and Ryabko B. Ya.* Eksperimental'nyj analiz generatorov psevdosluchajnyh chisel pri pomoshchi novogo statisticheskogo testa [Experimental analysis of pseudo-random number generators using a new statistical test]. Zhurnal Vychislitel'noj Matematiki i Matematicheskoj Fiziki, 2004, vol. 44, no. 5, pp. 766–770. (in Russian)

17. *Ryabko B. Ya. and Pestunov A. I.* “Stopka knig” kak novyj statisticheskij test dlya sluchajnyh chisel [Book Stack as a new statistical test for random numbers]. Problemy Peredachi Informacii, 2004, vol. 40, no. 1, pp. 73–78. (in Russian)
18. *Ryabko B. Ya., Monarev V. A., and Shokin Yu. I.* Novyj tip atak na blokovye shifry [A new type of attack on block ciphers]. Problemy Peredachi Informacii, 2005, vol. 41, no. 4, pp. 97–107. (in Russian)
19. *Monarev V. A.* Realizaciya novoj statisticheskoj ataki na blochnyj shifr [Implementation of a new statistical attack on a block cipher]. Vestnik SibGUTI, 2014, vol. 1, pp. 85–90. (in Russian)
20. *Lysyak A. S., Ryabko B. Ya., and Fionov A. N.* Analiz effektivnosti gradientnoj statisticheskoj ataki na blokovye shifry RC6, MARS, CAST-128, IDEA, Blowfish v sistemah zashchity informacii [Analysis of the effectiveness of gradient statistical attacks on block ciphers RC6, MARS, CAST-128, IDEA, Blowfish in information security systems]. Vestnik SibGUTI, 2013, vol. 1, pp. 85–109. (in Russian)
21. *Lerman L., Bontempi G., and Markowitch O.* A machine learning approach against a masked AES. J. Cryptogr. Eng., 2015, vol. 5, pp. 123–139.
22. *Hettwer B., Gehrer S., and Guneysu T.* Applications of machine learning techniques in side-channel attacks: a survey. J. Cryptogr. Eng., 2020, vol. 10, pp. 135–162.
23. *Szegedy C., Vanhoucke V., Ioffe S., et al.* Rethinking the inception architecture for computer vision // Proc. IEEE Conf. CVPR, Las Vegas, NV, USA, June 27–30, 2016, pp. 2818–2826.
24. *Monarev V. A. and Pestunov A. I.* Effektivnoe obnaruzhenie steganograficheski skrytoj informacii posredstvom integral’nogo klassifikatora na osnove szhatiya dannyh [Efficient steganography detection by means of compression-based integral classifier]. Prikladnaya Diskretnaya Matematika, 2018, no. 40, pp. 59–71. (in Russian)
25. *Monarev V. A. and Pestunov A. I.* Povyshenie effektivnosti metodov stegoanaliza pri pomoshchi predvaritel’noj fil’tracii kontejnerov [Enhancing steganalysis accuracy via tentative filtering of stego-containers]. Prikladnaya Diskretnaya Matematika, 2016, no. 2(32), pp. 87–99. (in Russian)
26. *Kodovsky J., Fridrich J., and Holub V.* Ensemble classifiers for steganalysis of digital media. IEEE Trans. Information Forensics and Security, 2010, vol. 7, no. 2, pp. 434–444.
27. *Pestunov A. I. and Perov A. A.* Programmnaya biblioteka dlya statisticheskogo analiza iterativnyh blochnyh shifrov [Software library for statistical analysis of iterative block ciphers]. Informacionnoe Protivodejstvie Ugrozam Terrorizma, 2015, vol. 24, pp. 197–202. (in Russian)