5. *Медведева Н. В., Титов С. С.* Описание неэндоморфных максимальных совершенных шифров с двумя шифрвеличинами // Прикладная дискретная математика. 2015. № 4 (30). С. 43–55.
6. *Медведева Н. В., Титов С. С.* Геометрическая модель совершенных шифров с тремя шифрвеличинами // Прикладная дискретная математика. Приложение. 2019. № 12. С. 113–116.
7. *Birkhoff G. D.* Tres observations sobre el algebra lineal // Revista Universidad Nacional Tucuman. 1946. Ser. A. V. 5. P. 147–151.

УДК 519.7 DOI 10.17223/2226308X/13/16

ПОСТРОЕНИЕ РАЗЛИЧИТЕЛЕЙ ДЛЯ ИТЕРАТИВНЫХ БЛОЧНЫХ ШИФРОВ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

А. А. Перов, А. И. Пестунов

Предлагается новый универсальный подход к построению атак-различителей на итеративные блочные шифры, подразумевающий использование нейронных сетей, предназначенных для классификации растровых изображений. Описываются два метода, основанных на идее представления шифртекстов после разного числа раундов шифрования в виде растровых изображений с последующим обучением нейронной сети распознавать эти изображения. Показано, что для ряда современных блочных шифров предлагаемый подход более эффективен, чем универсальные различители, основанные на статистических тестах.

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

В работе предлагается новый универсальный подход к построению атак-различителей на итеративные блочные шифры, где используются нейронные сети, предназначенные для классификации растровых изображений. Идея данного подхода возникла в результате наблюдения того, что преобразованный в растровое изображение (графический эквивалент) шифртекст имеет различную текстуру (паттерн) в зависимости от числа раундов. При этом с ростом числа раундов такая текстура становится менее выраженной и приближается к случайной.

В рамках этого подхода предлагаются два метода: «эталонный» и метод соседних раундов. В первом нейронная сеть используется для выявления различий в текстурах графических эквивалентов шифртекста при различном числе раундов и эталонной последовательности, неотличимой от случайных чисел. Второй метод предполагает выявление различий в текстурах графических эквивалентов соседних раундов и, что является его достоинством, не требует наличия эталонной последовательности, однако, забегая вперед, отметим, что «эталонный» метод оказался немного более эффективен. В экспериментах в качестве эталонной последовательности использован шифртекст полнораундового шифра AES256.

Для реализации предлагаемых методов необходимо выполнить процесс обучения свёрточной нейронной сети на графических эквивалентах шифртекстов (алгоритм 1).

Для формирования выборки выполняется шифрование на разном числе раундов, что даёт выборку выходных последовательностей блочных шифров с разными статистическими свойствами. На шагах 2–3 алгоритма 1 с помощью криптографической программной библиотеки «УНИБЛОКС-2015» выполняется шифрование в режиме

Алгоритм 1. Обучение нейронной сети для распознавания шифртекста после заданного числа раундов

1: **Функция** ОбучитьНейроннуюСеть($Cipher$, r, M)
   // *$Cipher$ — итеративный блочный шифр;*
   // *r — число раундов шифра;*
   // *M — размер обучающего множества.*
2: Сгенерировать M выборок с помощью шифра AES256 и получить $\tilde{\mathcal{Y}}^{\text{rand}} = (\tilde{y}_1^{\text{rand}}, \ldots, \tilde{y}_M^{\text{rand}})$.
3: Сгенерировать M выборок с помощью шифра $Cipher$ и получить $\tilde{\mathcal{Y}}^r = (\tilde{y}_1^r, \ldots, \tilde{y}_M^r)$.
4: Преобразовать множества выборок $\tilde{\mathcal{Y}}^{\text{rand}}$ и $\tilde{\mathcal{Y}}^r$ в изображения $\mathcal{Y}^{\text{rand}} = (y_1^{\text{rand}}, \ldots, y_M^{\text{rand}})$ и $\mathcal{Y}^r = (y_1^r, \ldots, y_M^r)$.
5: Обучить нейронную сеть различать изображения из обучающих выборок $\mathcal{Y}^{\text{rand}}$ и $\mathcal{Y}^r$.
6: **Вернуть** НейроннаяСеть^r(image), которая относит image к 0 (случайному) или 1 (r-раундовому шифртексту).

счётчика (CTR) [1]. В качестве входной последовательности для блочного шифра использованы последовательные числа 0, 1, 2, 3 и т. д.

На шаге 4 шифртексты преобразуются в формат растровых графических изображений с помощью разработанной программной утилиты на языке C++.

В процессе обучения нейронная сеть запоминает основные паттерны, характерные для шифртекстов на разном числе раундов, которые использует для последующей категоризации.

После обучения свёрточной нейронной сети выполняется распознавание шифртекстов. В зависимости от выбранного метода на контрольной выборке нейронная сеть сравнивает шифртексты на соседних раундах шифрования или шифртексты выбранного раунда с «эталоном» — полнораундовым AES256, подсчитывает процент верных решений при определении принадлежности элемента контрольной выборки к тому или иному множеству. С увеличением числа раундов шифрования и соответственно улучшением статистических свойств модель увеличивает значение E — число ошибок, допущенных моделью при определении принадлежности к тому или иному раунду на контрольной выборке. Алгоритм 2 описывает атаку-различитель.

С увеличением числа раундов ошибка при различении шифртекстов и эталонной случайной последовательности возрастает и стремится к 0,5. Алгоритм 3 описывает схему проведения экспериментов, в которых анализируется способность предлагаемого подхода различать шифртексты на примере «эталонного» метода.

Обоснование эффективности метода соседних раундов выполняется аналогично, за исключением того, что генерируются не выборки шифра AES256, а выборки x^r и x^{r+1}. Размер обучающей выборки выбирается нейронной сетью в зависимости от исходных параметров (в большей степени — от размера партии, то есть количества изображений, в которых нейронная сеть выполняет поиск общих признаков). Экспериментально определено, что 500 шифртекстов достаточно для обучения. Контрольная выборка составляет 20 % от обучающей. При этом процент ошибок нейронной сети на первых раундах выше (так как соседние раунды различимы между собой много меньше, чем при сравнении с эталонным шифртекстом), однако при достижении числа раундов, при котором обеспечиваются удовлетворительные статистические свойства, ошибка также сводится к 0,5.

Алгоритм 2. Атака-различитель

Функция РАСПОЗНАТЬШИФРТЕКСТ(x, $Cipher$, r)
// x — запрошенная в шифровальном устройстве выборка (генерируется в режиме CTR в сценарии chosen-plaintext attack);
// $Cipher$ — итеративный блочный шифр;
// r — число раундов шифра.
Выбрать размер обучающей выборки M.
НейроннаяСеть^r(image): = ОБУЧИТЬНЕЙРОННУЮСЕТЬ($Cipher$, r, M).
Представить выборку x в виде изображения image.
Result := НейроннаяСеть^r(image).
Если Result = 0, **то**
  вернуть «Выборка случайная»,
иначе
  вернуть «Выборка сгенерирована r-раундовым шифром».

Алгоритм 3. Схема проведения экспериментов

Функция ВЫЧИСЛИТЬОШИБКУ($Cipher$, r)
Выбрать размер обучающей выборки M.
НейроннаяСеть^r(image) := ОБУЧИТЬНЕЙРОННУЮСЕТЬ($Cipher$, r, M).
Выбрать количество контрольных выборок N.
Сгенерировать N контрольных выборок с помощью шифра AES256 и получить $\tilde{\mathcal{X}}^{\text{rand}} = (\tilde{x}_1^{\text{rand}}, \ldots, \tilde{x}_N^{\text{rand}})$.
Сгенерировать N контрольных выборок с помощью шифра $Cipher$ и получить $\tilde{\mathcal{X}}^r = (\tilde{x}_1^r, \ldots, \tilde{x}_N^r)$.
Преобразовать множества $\tilde{\mathcal{X}}^{\text{rand}}$ и $\tilde{\mathcal{X}}^r$ в изображения $\mathcal{X}^{\text{rand}} = (x_1^{\text{rand}}, \ldots, x_N^{\text{rand}})$ и $\mathcal{X}^r = (x_1^r, \ldots, x_N^r)$.
Экспериментально определить ошибки первого и второго рода:
$E_0 = \#\{x_i^{\text{rand}} : \text{НейроннаяСеть}^r(x_i^{\text{rand}}) = 1\}$, $E_1 = \#\{x_i^r : \text{НейроннаяСеть}^r(x_i^r) = 0\}$.
Вернуть E_0, E_1.

ЛИТЕРАТУРА

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

УДК 003.26 DOI 10.17223/2226308X/13/17

О СКРЫТОМ КОМПАКТНОМ СПОСОБЕ ХРАНЕНИЯ ДАННЫХ[1]

В. А. Романьков

Предлагается принципиально новый способ компактного хранения данных в скрытом виде. Каждое из этих данных может быть извлечено единообразным способом. Приводится сравнение с другими возможными способами такого хранения.

Ключевые слова: *данные, хранение, скрытость, компактность, доступ.*

[1]Исследование поддержано Программой фундаментальных научных исследований СО РАН I. 1.1.4, проект № 0314-2019-0004.