www.esa-conference.ru

Блочное шифрование с переменными ключами

Добрица Вячеслав Порфирьевич, доктор физико-математических наук, профессор
Верютина Кристина Геннадьевна, студент
Юго-Западный государственный университет (г. Курск)

В данной статье предложен метод формирования ключей для блочного алгоритма шифрования с применением искусственной нейронной сети. Каждый блок шифруется с использованием своего ключа, зависящего от предыдущего текста и шифротекста. Приводятся описание алгоритма и структура подобной системы.

Ключевые слова: *искусственные нейронные сети, блочное шифрование, переменные ключи, управление ключами, криптография.*

Введение

С развитием криптографии появилась возможность передавать информацию по открытым каналам связи, что позволяет сократить денежные затраты на реализацию передачи секретных данных по сравнению с использованием закрытых каналов. В настоящее время используются различные методы криптографической защиты информации. Одним из них является блочное шифрование.

1. Использование нейронных сетей для блочного шифрования в системах и их недостатки

Блочный шифр (block cipher)— это функция шифрования, которая применяется к блокам текста фиксированной длины. Данный способ шифрования имеет не высокую криптостойкость. Для ее повышения используются различные подходы [1, 2]. Рассмотрим некоторые из них.

В статье [1] доказано, что можно повысить криптостойкость блочного шифрования применением нейросетевого блока. В этом подходе существует возможность выбора закрытого ключа шифрования, который вырабатывается по короткому коду, сопровождающему сообщение. Увеличение времени использования этой системы в сравнении с жизненным циклом одного закрытого ключа происходит за счет их чередования. Однако существует нюанс, влияющий на криптостойкость данной системы – использование вспомогательных кодов, которые могут наталкнуть злоумышленника на понимание функционирования этой модели шифрования. Кроме того, может происходить накапливание шифротекстов с одинаковым кодом, что также может дать возможность злоумышленнику раскрыть ключ, соответствующий этому коду.

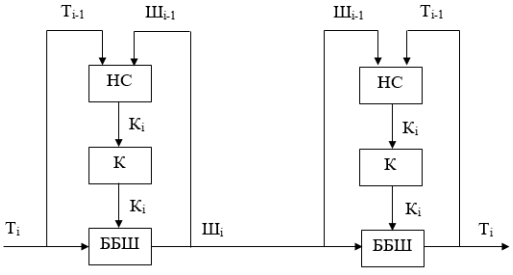

Рис. 1. Схема системы с меняющимися ключами в блочном шифровании

Где: T_i – текст i-го блока; $Ш_i$ – шифротекст i-го блока; НС – нейросеть выработки ключа; К – блок временного хранения ключа; ББШ – блок блочного шифрования; n – длина блока шифрования (n=64; 128; 256).

Использование двух нейросетей, синхронизирующихся по одинаковой базе (сигналам, подаваемым на вход), позволяет генерировать на выходе идентичные ключи [2]. Наличие шифратора, преобразующего информацию по правилам известным только абонентам, делает возможным сокрытие данных, обучающих НС. Недостатком этого подхода является кодирование текста одним ключом, что подвергает систему возможности вскрытия при большом объеме сообщения. Поэтому рассмотрим модель, в которой происходит вырабатывание нового ключа на каждый блок, поступающий на вход.

2. Блочное шифрование с переменными ключами

Количество входов и выходов НС определяется по длине блока шифрования: число входных нейронов сети – 2n, число выходных нейронов – n.

В начальном состоянии блоки К содержат какой-то ключ (он может быть сформирован при подаче последовательностей из 0 или 1 на вход НС). В дальнейшем каждый блок шифруется с использованием своего ключа, зависящего от предыдущего текста и шифротекста, которые идентичными не бывают, т.к. с каждой итерацией происходит шифрование текста новым сформированным ключом. Для ББШ может быть выбран любой из блочных шифров: перестановки, замены, DES, ГОСТ и т.д.

Требования к НС:

1)на вход подается последовательность из 0 и 1;

2)на выходе также последовательность из 0 и 1;

3)у абонентов НС идентичны;

4)наличие у НС 2-3 рабочих слоя с сигмоидальной функцией активации;

5)на выходе корректирующий слой.

На рисунке 2 представлена структура предлагаемой нейронной сети. Использовать следует НС многослойную, содержащую 2-3 рабочих слоя и с дополнительным корректирующим выходным слоем. Он необходим для того, чтобы происходило разбиение вершин n-мерного куба на два класса, отмеченных 0 и 1 соответственно, причем аргументы и сама функция меняются в пределах отрезка [0; 1] и во всех вершинах n-мерного куба, отмеченных единицей, она имеет значение 1, а в вершинах, отмеченных нулем, она имеет значение 0 [3, с. 15].

Существует теорема А.Н. Колмогорова, доказывающая, что любая непрерывная $f = (x_1, x_2, \dots, x_n)$ $f = (x_1, x_2, \dots, x_n)$ функция $f = (x_1, x_2, \dots, x_n)$, принимающая значения из отрезка [0;1], от n переменных, изменяющихся в этом же отрезке, может быть представлена в виде суперпозиции одноместных функций [4]. Поэтому для выхода из этой ситуации будем использовать сигмоидальную функцию активации на 2 и 3 рабочих слоях, в то время как на 4 слое – линейная.

ЕВРАЗИЙСКОЕ НАУЧНОЕ ОБЪЕДИНЕНИЕ
EURASIAN SCIENTIFIC ASSOCIATION
www.esa-conference.ru

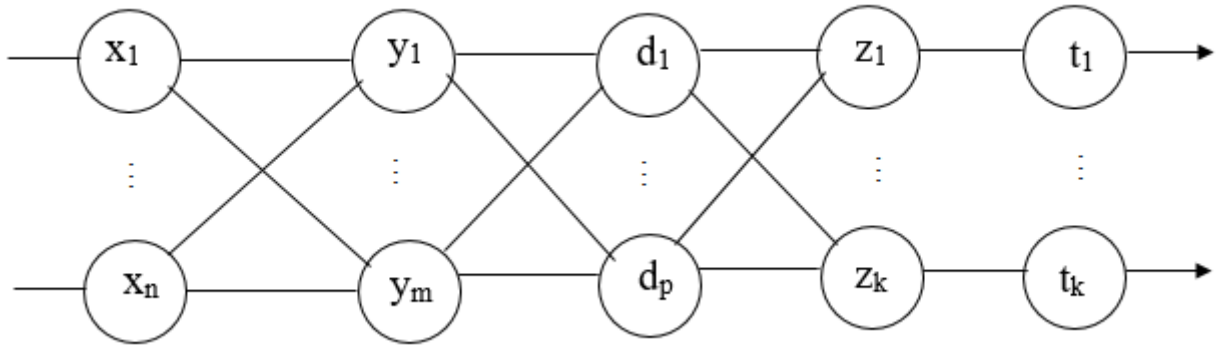

Рис. 2. Структура предлагаемой НС

А на корректирующем 5 слое используется пороговая функция активации:

$$t_j = signz_k = \begin{cases} 1, z_k > 0; \\ 0, z_k < 0. \end{cases} \quad (1)$$

НС до корректирующего выходного слоя может задаваться достаточно произвольно.

При «сбое» формирования ключей необходимо вернуть систему в исходное положение, запустив текст из 0.

Процесс обучения НС можно проводить по алгоритму обратного распространения ошибки. Исходные весовые коэффициенты задаются случайным образом. Но можно эту сеть задать случайным выбором весовых коэффициентов для рабочих слоев и в этом случае перед использованием нейронной сети провести предварительное тестирование, чтобы убедиться, что смена ключей происходит на каждом шаге, т.е. нейросеть не задает функцию с малым числом выходных значений.

Любой из абонентов может быть отправляющей или принимающей стороной, потому что они будут иметь идентичные нейросети, необходимые для генерации одинаковых секретных ключей.

Заключение

«Секретом» является сама нейросеть. Она может быть выполнена на внешнем носителе (либо программным, либо аналоговым способом) и неизвестна как самим пользователям (в расчете на «человеческий фактор» в потере секретности), так и, естественно, злоумышленнику.

Атакующему для криптоанализа одного шифроблока мало, так как при следующей итерации формируется новый ключ. И даже если этот ключ будет разгадан, то он больше не используется, и потому «бесполезен» для прочтения всего текста.

Литература:

1. Добрица В.П., Липунов А.А. Нейросетевой шифратор текстов: Известия Юго-Западного государственного университета, 2011, № 5 (38), часть 1, С. 93-97.
2. Добрица В.П., Сапельченков П.А., Жильцов В.Н. Распределение ключей с использованием искусственной нейросети: Нейрокомпьютеры: разработка и применение. 2014, № 6, с. 19-21.
3. Добрица В.П., Захарина А.Ю., Уалиев Н.С. Повышение стойкости блочного шифрования применением нейросетевого блока: Нейрокомпьютеры: разработка, применение, № 6, 2015, с. 14 – 17.
4. Колмогоров А.Н. Представление непрерывных функций многих переменных суперпозицией функций одной переменной и сложением: ДАН СССР. 1958. № 5. С. 953–956
5. Добрица В.П., Канонников Д.С. Нейросетевой подход к распределению ключей: Проблемы информационной безопасности. Компьютерные системы. 2010, № 3, с. 52-54.
6. Добрица В.П, Волокитин С.С. Блочный шифр на основе нейронной сети: Нейрокомпьютеры: разработка, применение, № 6, 2014, с.16,53 – 18,55
7. Добрица В.П., Нургабыл Д. Н., Уалиев Н.С. Существование классифицирующей нейронной сети для произвольного разбиения вершин n-мерного куба на два множества: Нейрокомпьютеры: разработка, применение, № 6, 2014, с.12,48 – 15,52