УДК 681.325.3

М. Плонковски, аспирант

ИСПОЛЬЗОВАНИЕ НЕЙРОННЫХ СЕТЕЙ В ОПЕРАЦИЯХ НАД ХЕШ-ФУНКЦИЯМИ

The article is devoted to the offered architecture of a neural network which works by criteria of hash-function. The network consists of three layers: input, hidden and output. These layers realize following operations: hashing, dis-persion and compression of input bits. The model of a network can be used in cryptographic systems for an ex-change of confidential data. One of the main feature of this model is greater complexity of return size transition function calculation, and also greater freedom choice of that type of function that is advantage at realization of the information cryptographic transformation methods.

Введение. В [1] предложен новый протокол обмена ключами, использующий взаимное обучение нейронных сетей и базирующийся на известной архитектуре TPM (Tree Parity Machine).

Классический метод согласования ключей и обмена ключами (Diffie-Hellman) основывается на трудности вычисления дискретного логарифма. Идея применения нейросетевых технологий для криптографических приложений связана с проблемой обмена ключами через незащищенные каналы передачи.

В [2] проанализирована возможность расширения упомянутого протокола за счет использования комплексных чисел в процессе обучения сетей. Ниже будут описаны новые результаты в этом направлении.

Как известно, взаимное обучение двух сетей приводит к синхронизации их векторов весов (весовых коэффициентов). Протокол обмена ключами, который используется в нейросетевых криптографических технологиях, опирается на синхронном обучении сетей со стороны отправителя и получателя сообщений. Процесс обучения двух нейронных сетей с применением их общих параметров ведется до появления так называемых идентичных весовых коэффициентов (векторов весов). Сети обмениваются между собой выходными и входными параметрами; при этом секретными должны оставаться внутренние значения весовых коэффициентов. Следовательно, значения весовых коэффициентов могут использоваться как секретные ключи в процессе передачи информации по незащищенным каналам.

Хеш-функции – это существенные элементы криптографических систем. Они применяются в парольной охране компьютерных систем, в аутентификации данных, а также в электронной цифровой подписи. Роль этого типа функции состоит в создании коротких последовательностей данных (установленной длины) на основании длинных входных последовательностей (произвольной длины). Сгенерированные сокращения должны быть уникальными и характерными для данного сообщения.

От хеш-функций требуется, чтобы они были чувствительными к изменениям бит в оригинальном тексте (даже один измененный бит сообщения должен вызвать смену многих битов сокращения), а также были слабо коррелированы (вероятность появления двух сообщений с идентичными функциями должна быть очень малой) [1].

Нужно заметить, что признание функции неопасной для криптографических применений в принципе основывается на устойчивости к известным криптоаналитическим атакам, а не на математических методах, гарантирующих невозможность их взлома. В последнее время найдены серьезные недостатки многих хеш-функций, признаваемых до сих пор неопасными (MD2, MD4, SHA, а в последнее время – также MD5). Поэтому важным и актуальным является поиск новых методов генерации хеш-функции. Настоящая статья посвящена одному из аспектов данной проблемы.

Хеш-функции на основе нейронных сетей. Биты, содержащиеся во входных последовательностях, преобразованных через нейронные сети, могут подвергнуться перемешиванию и рассеиванию, что предусматривается реализацией процедур кодирования передаваемых сообщений. С другой стороны, сети имеют свойство односторонности. Оба этих фактора допускают возможность генерации хеш-функции, основанной на использовании технологии нейронных сетей.

В [2] предложена архитектура нейронной сети, которая работает по критериям хеш-функции. Эта сеть состоит из трех слоев: входного, скрытого и выходного. Эти слои реализуют следующие операции: перемешивание, рассеивание и сжатие входных битов. Входные и выходные векторы слоев принимают соответственно следующими (попарно): $P = [P_0P_1...P_{31}]$, $C = [C_0C_1...C_7]$, $D = [D_0D_1...D_7]$ и $H = [H_0H_1...H_3]$.

Выход сети H определяется следующим образом:

$$H = f_2(W_2D + B_2) = f_2(W_2f_1(W_1C + B_1) + B_2) =$$
$$= f_2(W_2f_1(W_1f_0(W_0P_0 + B_0) + B_1) + B_2), \quad (1)$$

где f_i – функция перехода; W_i – вектор весов; B_i – смещение (bias).

Функция перехода f_i находится следующим способом:

$$X(k+1) = f(X(k), Q) =$$
$$= \begin{cases} X(k)/Q, & 0 \le X(k) < Q, \\ (X(k)-Q)/(0.5-Q), & Q \le X(k) < 0.5, \\ (1-Q-X(k))/(0.5-Q), & 0.5 \le X(k) < 1-Q, \\ (1-X(k))/Q, & 1-Q \le X(k) \le 1, \end{cases} \quad (2)$$

где Q – это числовой параметр, принимающий значения в диапазоне [0, 0.5].

Для параметра Q, принадлежащего вышеуказанному диапазону, функция f – это функция хаоса. Если мы сделаем много итераций вышеуказанной функции, то в результате получим величину, гарантирующую высокую степень случайности и практическую невозможность обратного преобразования, т. е. определения входного значения.

Выход первого слоя устанавливается следующим образом:

$$C = f^T\left(\begin{bmatrix} \sum_{i=0}^{3} w_{0,i}P_i + b_{0,0} \\ \sum_{i=4}^{7} w_{0,i}P_i + b_{0,1} \\ \vdots \\ \sum_{i=28}^{31} w_{0,i}P_i + b_{0,7} \end{bmatrix}, Q_0\right) =$$
$$= \begin{bmatrix} f^T(\sum_{i=0}^{3} w_{0,i}P_i + B_{0,0}, Q_0) \\ f^T(\sum_{i=4}^{7} w_{0,i}P_i + B_{0,1}, Q_0) \\ \vdots \\ f^T(\sum_{i=28}^{31} w_{0,i}P_i + B_{0,7}, Q_0) \end{bmatrix} = \begin{bmatrix} C_0 \\ C_1 \\ \vdots \\ C_7 \end{bmatrix}, \quad (3)$$

где T – это количество итераций (не менее 50).

Принимается, что входные величины функции f принадлежат диапазону [0, 1], а все операции выполняются по mod 1 и определяются следующим образом:

$$a \bmod 1 = \begin{cases} a, & 0 \le a < 1, \\ a-1, & 1 \le a < 2. \end{cases} \quad (4)$$

Подобным образом вычисляются выходные величины других слоев:

$$D = f_1(W_1C + B_1) = f(W_1C + B_1, Q) =$$
$$= \begin{bmatrix} f(\sum_{i=0}^{7} w_{1,0,i}C_i + B_{1,0}, Q_1) \\ f(\sum_{i=0}^{7} w_{1,1,i}C_i + B_{1,1}, Q_1) \\ \vdots \\ f(\sum_{i=0}^{7} w_{1,7,i}C_i + B_{1,7}, Q_1) \end{bmatrix} = \begin{bmatrix} D_0 \\ D_1 \\ \vdots \\ D_7 \end{bmatrix}, \quad (5)$$

$$H = f_2(W_2D + B_2) = f^T(W_2D + B_2, Q_2) =$$
$$= \begin{bmatrix} f^T(\sum_{i=0}^{7} w_{2,0,i}D_i + B_{2,0}, Q_2) \\ f^T(\sum_{i=0}^{7} w_{2,1,i}D_i + B_{2,1}, Q_2) \\ \vdots \\ f^T(\sum_{i=0}^{7} w_{2,3,i}D_i + B_{2,3}, Q_2) \end{bmatrix} = \begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_3 \end{bmatrix}. \quad (6)$$

Предлагаемая архитектура нейронной сети может исполнять роль хеш-функции. Она способна преобразовывать входное сообщение длиной 1024 бита до 128 бит. Входная последовательность, пронормированная величиной 2^{32}, попадает в диапазон [0, 1].

Для генерации ключей W_0, B_0, Q_0, W_1, B_1, Q_1, W_2, B_2, Q_2 используется следующий алгоритм: ключ $K = k_0k_1...k_{127}$ делится на четыре подключа: $K_0 = k_0k_1...k_{31}$, $K_1 = k_{32}k_{33}...k_{63}$, $K_2 = k_{64}k_{65}...k_{95}$, $K_3 = k_{96}k_{97}...k_{127}$. Затем осуществляется последовательность следующих операций:

$$X_0(k) = f^{T+k}(K_0, K_1),$$
$$X_1(k) = f^{T+k}(K_2, K_3), \quad (7)$$
$$K_S(k) = (X_0(k), X_1(k)) \bmod 1.$$

Результат вышеуказанных операций $K_S(k)$ (k = 0, 1, ..., 150) будет k-м подключом.

Хеш-функции на основе комплексных чисел и нейросетевых преобразований. Нейронные сети, основанные на комплексных числах, могут быть использованы в протоколе согласования ключа. Благодаря специфике алгебры комплексных чисел они обеспечивают более высокий уровень безопасности, чем их классические эквиваленты [3]. Вторым существенным аргументом является большая свобода при определении разного рода структур, встречающихся в данной архитектуре. Это также позволяет увеличить безопасность системы [4].

Вся структура нейронной сети, основанная на комплексных числах, аналогична структуре, базирующейся на вещественных числах. Различие касается функции перехода, которая должна гарантировать односторонность преобразований. Для функции перехода f, определенной в предыдущей части статьи, трудно установить обратную, но можно создать карту

переходов и хранить ее в индексированном массиве. Единственная проблема связана с выбором размера массива. Он должен быть не меньше чем $2^{32}\times2^{32}$, что обеспечивает хранение всех возможных состояний переходов. В современных компьютерах такие параметры можно создать.

В случае функции перехода, оперирующей на комплексных числах, размер массива должен соответствовать параметрам: $2^{32}\times2^{32}\times2^{32}\times2^{32}$. Такой гигантский размер пока недоступен ни одной известной компьютерной системе.

Проанализируем далее три функции, способные исполнять роль функции перехода в архитектурах нейронных сетей, основанных на комплексных числах. Первая из предложенных функций базируется на уравнении, определяющем совокупность Юлии, которая является одной из важных в теории хаоса. Именно в ее определении применяется следующая рекурсивная последовательность:

$$\begin{aligned} z_0 &= p, \\ z_{n+1} &= z_n^2 + c, \end{aligned} \tag{8}$$

где z_i, p и $c \in \Omega$ (Ω – множество комплексных чисел); p – входной параметр, в качестве параметра Q будет использоваться переменная c.

Вторая функция основывается на уравнении Даффинга (Duffing), графическое отображение которого представлено на рисунке. Карта хаоса найдена следующим способом:

$$\begin{aligned} x_{n+1} &= y_n, \\ y_{n+1} &= -bx_n + ay_n - y_n^3. \end{aligned} \tag{9}$$

В этом уравнении все переменные – действительные числа, а пары (x_i, y_i) отождествлены с точками плоскости. Из-за однозначности функции между точками плоскости и комплексными числами пара (x_i, y_i) может быть отождествлена с комплексным числом (в части действительной – x_i и в части мнимой – y_i). Параметром этой функции будет пара (a, b), являющаяся также комплексным числом.

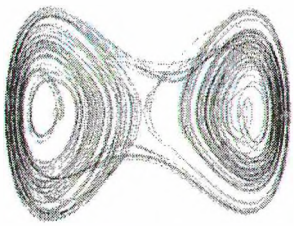

Рисунок. Бессвязное поведение точек на основе уравнения Даффинга

Третья функция определяется по уравнению Шенона (Henon) следующим образом:

$$\begin{aligned} x_{n+1} &= y_n + 1 - ax_n^2, \\ y_{n+1} &= bx_n. \end{aligned} \tag{10}$$

Нахождение переменных x_i и y_i, а также параметров a и b аналогично случаю использования уравнения Даффинга.

Заключение. В статье обсуждены некоторые аспекты применения нейронных сетей как хеш-функции. Предложено видоизменение используемых нейронных сетей, основанное на комплексных числах. Данная модель характеризуется большой сложностью вычисления обратной величины функции перехода, а также большой свободой выбора этого типа функции, что является достоинством при реализации методов криптографического преобразования информации.

Литература

1. Menezes, J. Handbook of Applied Cryptography / J. Menezes, P. C. van Oorschot, S. A. Vanstone. – CRC Press, 1997.

2. Lian, S. Secure hash function based on neural network / S. Lian, J. Sun, Z. Wang // Neurocomputting. – 2006. – Vol. 69. – P. 2346–2350.

3. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологий / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI, Физ.-мат. науки и информ. – 2005. – Вып. XIII. – С. 161–164.

4. Płonkowski, M. Algebraic aspects of mutual learning of neural networks / M. Ponkowski // New Electrical and Electronic Technologies and Their Industrial Implementation. – Zakopane, Poland, 21–24 June 2005.