УДК 681.3.006

К. В. Чуриков, ассистент (БГТУ)

МЕТОДЫ ВЫЧИСЛЕНИЯ И АНАЛИЗА ХЕШ-ФУНКЦИЙ НА ОСНОВЕ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

В статье рассмотрены особенности методов использования рекурсивных последовательностей в функциях перехода нейронных сетей. Такой подход позволяет сделать практически невозможным обратное преобразование и тем самым увеличивает криптостойкость хеш-функций. Предложена модель нейронной сети на основе алгебры комплексных чисел, которая использует функции хаоса в качестве функций перехода. Проведен вероятностный анализ стойкости информационной системы в виде двух связанных между собой нейронных сетей на основе предложенной архитектуры к различным видам атак на нее.

The article describes the features of the use of recursive sequences in the transition function of neural networks. This approach allows us to make it virtually impossible inverse transform, and thereby increases the cryptographic strength of hash functions. A model of neural network based on the algebra of complex numbers, which uses the functions of the chaos as the transition functions. A probabilistic analysis of the stability of the information system in the form of two interconnected neural networks based on the proposed architecture for different types of attacks on it.

Введение. В настоящее время информационные технологии активно внедряются в повседневную жизнь. Вместе с огромной пользой и, казалось бы, неограниченными возможностями новые технологии вызывают и новые проблемы. Одной из них является проблема защиты информации от несанкционированного доступа. В связи с этим одновременно с появлением информационных и компьютерных технологий начали разрабатываться и технологии защиты информации, создание которых более актуально, чем развитие непосредственно информационных технологий. Технология использования искусственных нейронных сетей для моделирования криптографических систем передачи информации является новейшим и очень перспективным направлением в области защиты информации.

Хеш-функция преобразует входной массив данных произвольной длины в выходную битовую строку фиксированной длины. Такие преобразования называются хешированием, или сверткой, а их результаты называют хешем, хеш-кодом, или дайджестом сообщения (англ. message digest).

Существует множество алгоритмов хеширования с различными характеристиками (разрядность, вычислительная сложность, криптостойкость и т. п.). Выбор той или иной хеш-функции определяется спецификой решаемой задачи. Простейшими примерами хеш-функций могут служить контрольная сумма или CRC.

В общем случае однозначного соответствия между исходными данными и хеш-кодом нет. В связи с этим существует множество массивов данных, дающих одинаковые хеш-коды – так называемые коллизии. Вероятность возникновения коллизий играет немаловажную роль в оценке «качества» хеш-функций. Основными требованиями, предъявляемыми к хеш-функции, являются хорошее перемежение данных и быстрый алгоритм вычисления.

Существуют следующие области применения хеш-функций:

1. Сверка данных. В общем случае эту область применения можно описать как проверку информации на идентичность оригиналу без его использования. Для сверки используется хеш-значение проверяемой информации. Различают два основных направления такого применения:

а) проверка на наличие ошибок. Например, контрольная сумма может быть передана по каналу связи вместе с основным текстом;

б) проверка парольной фразы. В большинстве случаев на целевых объектах хранятся не парольные фразы, а лишь их хеш-значения.

2. Ускорение поиска данных. Например, при записи текстовых полей в базе данных может рассчитываться их хеш-код. В этом случае данные помещаются в раздел, ему соответствующий. Тогда при поиске данных необходимо сначала вычислить хеш-код текста, после чего станет известно, в каком разделе информацию нужно искать, т. е. процесс поиска упрощается.

3. Криптографические хеш-функции. Среди множества существующих хеш-функций принято выделять криптографически стойкие, применяемые в криптографии. Криптостойкая хеш-функция прежде всего должна обладать стойкостью к коллизиям двух типов:

а) для заданного сообщения должно быть практически невозможно подобрать другое сообщение, имеющее такой же хеш. Это свойство также называется необратимостью хеш-функции;

б) должно быть невозможно подобрать пару сообщений, имеющих одинаковый хеш.

Поскольку в нейронных сетях при использовании в качестве функций перехода рекурсивных последовательностей или функций хаоса нет однозначного соответствия между входными и выходными данными, их можно использовать для генерации хеш-кода. Способность данных сетей к взаимообучению и использованию алгебры комплексных чисел повышает уровень криптостойкости системы. Последние особенности являются предметом анализа в данной статье.

Основная часть. Как правило, криптографическая хеш-функция является конкатенацией различных составных частей или блоков, т. е. хеш-функция H есть соединение блоков h_i:

$$H = h_1 + h_2 + ... + h_i.$$

В современных системах i меняется от 3 до 6, причем вычисление каждого последующего блока хеш-функции зависит не только от данных, но и от значений предыдущих блоков:

$$h_i = F(M,\ h_i - 1),\ \ j = 2...i.$$

Искусственная нейронная сеть позволяет перемешивать, рассеивать и сжимать входную последовательность бит. Такое преобразование обеспечивает свойство односторонности. Это допускает возможность генерации хеш-функций, основанной на использовании технологии нейронных сетей. Сеть, работающая по критериям хеш-функции, состоит из множества нейронов, которые соединены между собой в слои произвольным образом, и реализует тем самым преобразования и сжатие входной информации. Также стоит отметить, что, в отличие от нейронных сетей, выполняющих обработку информации, сеть, выполняющая роль хеш-функции, может обладать односторонней функцией перехода, для которой не обязательно знать обратное значение. Следовательно, различные варианты хеширования обеспечиваются как коэффициентами связей между нейронами, видом функции перехода, так и самой архитектурой сети.

Для увеличения криптографической стойкости хеш-функций в алгебре нейронной сети используются комплексные величины. Вся структура нейронной сети, основанная на комплексных числах, аналогична структуре, базирующейся на действительных числах.

Условно в сети можно выделить три слоя: входной, скрытый и выходной. Во входном слое X последовательность бит проецируется на множество комплексных чисел:

$$z = \begin{cases} 1 + i, x = 1, \\ -1 - i, x = 0. \end{cases}$$

Скрытый слой Z реализует непосредственно саму функцию хеширования. Выход каждого нейрона слоя Z есть функция перехода взвешенной суммы его входов. Функция перехода может иметь различный вид [1]. Отличительной особенностью каждой из них является то, что в их основе лежит какая-либо рекурсивная функция $x_i = f(x_i - 1)$.

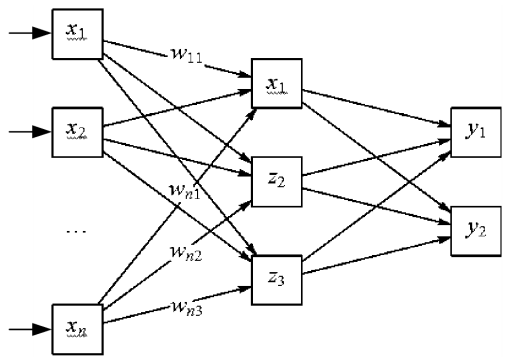
Таким образом, рекурсивная функция – это числовая функция $f(x_i)$ числового аргумента, которая в своей записи содержит себя же. Такая запись позволяет вычислять значения $f(x_i)$ на основе предыдущих значений функции $f(x_i - 1)$, $f(x_i - 2)$, ..., подобно рассуждению по индукции. Чтобы вычисление завершалось для любого x_i, необходимо, чтобы для некоторых x_i функция была определена нерекурсивно (например, для $x_{0,1}$).

Выходной слой Y преобразует комплексные величины скрытого слоя Z в последовательность бит. Переходная функция имеет вид

$$f(z) = (a \arg(z)) \bmod 2.$$

Таким образом, предложена модель нейронной сети (рисунок), которая способна преобразовывать входное сообщение любой длины до желаемого количества бит.

Генерация весовых коэффициентов синаптических связей осуществляется случайным образом. Сгенерированные веса являются ключом сети и не изменяются в процессе работы.



Модель нейронной сети,
выполняющей хеширование

Таким образом, рассмотрена возможность использования в функциях перехода рекурсивных последовательностей, основанных на комплексных числах. Это позволяет сделать практически невозможным нахождение обратного значения и тем самым увеличивает криптостойкость хеш-функций.

Поскольку атака методом грубой силы (полным перебором всех ключей) возможна для всех типов криптографических алгоритмов, то она может быть применена и для данного

алгоритма и может являться для него единственной существующей. Способы ее оценки основываются на вычислительной сложности, которая затем может быть выражена во времени, денежных затратах, и требуемой производительности вычислительных ресурсов. Эта оценка пока является максимальной и минимальной одновременно.

Дальнейшее исследование алгоритма с целью поиска уязвимостей включает оценки стойкости по отношению к известным криптографическим атакам (линейный криптоанализ, дифференциальный криптоанализ и более специфические). Эти оценки могут понизить известную стойкость. Например, для многих симметричных шифров существуют слабые ключи и S-блоки, применение которых снижает криптографическую стойкость. Также важным способом проверки стойкости являются атаки на реализацию, выполняемые для конкретного программно-аппаратного комплекса.

Чем более длительным и экспертным является анализ алгоритма и реализаций, тем более достоверной можно считать его стойкость. В нескольких случаях длительный и внимательный анализ приводил к снижению оценки стойкости ниже приемлемого уровня.

За прошедшее время установлено, что все атаки на алгоритмы хеширования являются коллизионными. Они относятся в основном к цифровым подписям приложений, когда атакующий имеет доступ к неподписанному документу.

Как упоминалось выше, криптостойкая хеш-функция прежде всего должна обладать стойкостью к коллизиям двух типов:

– пусть дано сообщение M и его хеш-значение $H(M)$. Тогда путем вычисления невозможно определить M', такое что $H(M) = H(M')$;

– путем вычисления невозможно найти два произвольных сообщения M и M', для которых $H(M) = H(M')$.

Для атаки на однонаправленные хеш-функции используют два метода [2]. Первый направлен на взлом первого рода, т. е. по известному значению хеш-функции $H(M)$ противник хочет создать другой документ M', такой что $H(M') = H(M)$. Другой направлен на коллизию второго рода: противник хочет найти два случайных сообщения M и M', таких что $H(M) = H(M')$.

Предположим, что однонаправленная хеш-функция надежна и лучшим методом ее вскрытия является перебор всех значений. Выход этой хеш-функции – m-разрядное число. Тогда количество выходных значений хеш-функции H равно $n = 2^m$.

Обозначим $P(n, k)$ – вероятность того, что для конкретного значения X и хотя бы для одного Y_i из значений $Y_1, \ldots, Y_k$ выполняется равенство $H(X) = H(Y)$. Для одного Y вероятность того, что $H(X) = H(Y)$, равна $1 / n$. Значит, вероятность того, что $H(X) \neq H(Y)$, равна $(1 - 1 / n)$. Если создать k значений, то вероятность того, что ни для одного из них не будет совпадений, равна произведению вероятностей, соответствующих одному значению, т. е. $(1 - 1 / n)^k$. Следовательно, вероятность, по крайней мере, одного совпадения равна $1 - (1 - 1 / n)^k$.

По формуле бинома Ньютона находим

$$(1-a) = 1 - ka + k\frac{k-1}{2!}a^2 - \ldots \approx 1 - ka,$$

$$1 - \left(1 - \frac{1}{n}\right)^k \approx 1 - \left(1 - \frac{k}{n}\right) = \frac{k}{n}.$$

Приравняв $P(n, k)$ к 0,5, получим

$$k = \frac{n}{2} = 2^{m-1}.$$

Таким образом, для нахождения сообщения M, которое хешируется к заданному значению $H(M)$, потребовалось бы хеширование 2^{m-1} случайных сообщений. Вероятность взлома хеш-функции при этом равна $1/2^{m-1} = 2^{1-m}$.

Также возможны различного рода атаки, основанные на «парадоксе дня рождения».

Возможна следующая стратегия.

1. Злоумышленник создает $2^{m/2}$ вариантов сообщения, каждое из которых имеет некоторый определенный смысл. Он подготавливает такое же количество сообщений, каждое из которых является поддельным и предназначено для замены настоящего сообщения.

2. Два набора сообщений сравниваются в поисках пары сообщений, имеющих одинаковый хеш-код. Вероятность успеха в соответствии с «парадоксом дня рождения» больше чем 0,5. Если соответствующая пара не найдена, то создаются дополнительные исходные и поддельные сообщения до тех пор, пока не будет найдена пара.

3. Атакующий предлагает отправителю исходный вариант сообщения для подписи. Эта подпись может быть затем присоединена к поддельному варианту для передачи получателю. Поскольку оба варианта имеют один и тот же хеш-код, будет создана одинаковая подпись, злоумышленник будет уверен в успехе даже без ключа шифрования.

Таким образом, если используется 64-битный хеш-код, то необходимая сложность вычислений составляет порядка 2^{32}. Следовательно, вероятность взлома хеш-функции $H(M)$ первым методом ниже, чем вторым.

Нейронные сети, основанные на комплексных числах, благодаря специфике алгебры

комплексных чисел, обеспечивают более высокий уровень безопасности [3, 4]. Второе достоинство – это большая свобода при определении разного рода вспомогательных структур, встречающихся в данной архитектуре, в частности различных функций перехода. Они также позволяют увеличить безопасность системы [5].

Как указано выше, структура нейронной сети, базисом которой является алгебра комплексных чисел, аналогична структуре, основанной на действительных числах. В случаях хеширования сообщений изменение будет касаться пороговой функции (перехода), которая должна гарантировать односторонность. Функция перехода f определяется формулой

$$X(k+1) = f\left(X(k),\ Q\right) =$$

$$= \begin{cases} \dfrac{X(k)}{Q}, & 0 \le X(k) < Q, \\ \dfrac{\left(X(k)-Q\right)}{\left(0{,}5-Q\right)}, & Q \le X(k) < 0{,}5, \\ \dfrac{(1-Q-X(k))}{(0{,}5-Q)}, & 0{,}5 \le X(k) < 1-Q, \\ \dfrac{(1-X(k))}{Q}, & 1-Q \le X(k) \le 1, \end{cases}$$

где f – функция перехода; Q – это параметр из промежутка (0; 0,5).

Для параметра Q, принадлежащего вышеуказанному промежутку, функция f – это функция хаоса. Если выполнить большое количество итераций вышеназванной функции, то в результате получится величина, гарантирующая случайность и невозможность возвращения к входной величине.

При использовании однонаправленных функций перехода возможна атака создания карт переходов, хранимых в массиве. Она позволяет для каждой выходной величины определить множество возможных входных величин. Размерность данного массива составляет $2^{32}\times2^{32}$ для сети, использующей алгебру целых чисел, и $2^{32}\times2^{32}\times2^{32}\times2^{32}$ для сети, основанной на комплексных числах. Это гигантский размер и его хранение невозможно в ближайшем будущем ни в одной из доступных компьютерных систем.

Заключение. Проведен анализ функций перехода элементов нейронной сети на основе рекурсивных последовательностей. Данное исследование характеризуется большой сложностью вычисления обратного значения, что является достоинством при реализации методов криптографического преобразования информации.

Предложенный метод отличается от известных использованием функций хаоса в качестве функций перехода. Благодаря их специфике возможна программная реализация математических операций в арифметике целых чисел (в известных решениях необходимо было использовать числа с плавающей запятой), что обеспечивает большее быстродействие выполнения операций.

Таким образом, представленное решение позволяет создавать более гибкие криптографические системы, что допускает выбор оптимальных решений. Кроме того, предложенное решение существенным образом увеличивает безопасность криптографических систем на основе нейросетевых технологий.

Литература

1. Плонковски, М. Использование нейронных сетей в операциях над хеш-функциями / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI, Физ.-мат. науки и информатика. – 2005. – Вып. XIII. – С. 169–171.

2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. – М.: ТРИУМФ, 2002. – 816 с.

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

4. Kinzel, W. Theory of Interacting Neural Networks / W. Kinzel. – 2002. – cond-mat/0204054.

5. Plonkowski, M. Algebraic aspects of mutual learning of neural networks / M. Plonkowski // New Electrical and Electronic Tecnologies and Their Industrial Implementation, Zakopane, Poland, 21–24 June. – Zakopane, 2005. – P. 125–127.

Поступила 26.02.2011