АНАЛИЗ СИНХРОНИЗАЦИИ НЕЙРОННЫХ СЕТЕЙ В ПРИКЛАДНОЙ КРИПТОГРАФИИ

Урбанович П. П., Бирюк И. А., Плонковски М. Д.
Кафедра информационных систем и технологий, Белорусский государственный технологический университет, Минск, Республика Беларусь
Люблинский католический университет Яна Павла II, Люблин, Польша
pav.urb@yandex.by, plomyk@kul.pl
E-mail:

Рассматриваются важные аспекты использования нейросетевых технологий в задачах согласования криптографических ключей и вычисления хеш-функций. Архитектура сетей строится на основе известной древовидной машины четности Кантера-Кинцеля. Авторами доклада ранее предложена идея расширения используемой алгебры: действительные числа дополнены комплексными, а также кватернионами и октонионами. Это значительно повышает криптостойкость системы, но усложняет процесс взаимного обучения сетей. Приведены экспериментальные результаты и параметры этого процесса.

Введение

Современные информационные системы с повышенным уровнем безопасности строятся, в основном, на основе асимметричной криптографии и хеш-преобразований с требуемым уровнем необратимости. Однако главным недостатком асимметричных криптосистем является сложность математических операций, что значительно увеличивает время выполнения вычислений. Поэтому, по-прежнему все еще достаточно часто используются симметричные криптосистемы. Проблема создания быстрых протоколов согласования ключей до сих пор остается актуальной. Указанные обстоятельства вызвали интерес к разработке новых криптографических методов, не использующих в своей конструкции теорию чисел.

Использование в хеш-алгоритме Keccak входа и выхода переменной длины может применяться для генерации симметричных ключей из паролей, из протоколов согласования ключа по асимметричным алгоритмам.

Использование искусственных нейронных сетей (ИНС) для решения задач защиты информации впервые предложено И. Кантером и В. Кинцелем [1]. Развитием общей идеи стала известная архитектура TPM (англ. Tree Parity Machine, древовидная машина четности). При этом изначально функционирование TPM предусматривало использование целых действительных чисел как поля для описания и анализа процессов в сети.

Целью данного доклада является анализ процесса сходимости (синхронизации) ИНС на основе расширенной алгебры.

I. Характеристика и параметры архитектуры TPM

Архитектура TPM состоит из K независимых персептронов, каждый из которых характеризуется N-элементным вектором весов ($[w_{k_1}$, w_{k_2}, ..., $w_{k_N}]$, где $1 \leq \mathrm{k} \geq \mathrm{K}$).

Коэффициенты этих векторов – это целые числа из интервала $[-L, L]$. Входы персептронов составляет K N-элементных векторов ($[x_{k_1}$, x_{k_2}, ...,x_{k_N}], где $x_{k_i} \in [-1, 1]$.

Выходы нейронов составляют K значений ($[z_1$, z_2, ..., $z_k]$, которые равны сумме произведений элементов векторов входных значений на соответствующие элементы векторов весов [2].

Для решения задачи согласования ключевой информации между двумя сторонами применяются две идентичные сети. Все структурные элементы (как и в других криптографических системах) известны. Секретными элементами, на которых основывается криптостойкость системы – это начальные состояния векторов весов. Процесс взаимного обучения сетей или синхронизации начинается с инициализации векторов весов обеих сетей. Их начальное состояние, сгенерированное случайным образом, остается секретным на протяжении всего процесса обучения. Каждый шаг синхронизации начинается с подачи на входы обеих сетей определенного двоичного вектора, вычисления выходного значения сети и обмена выходными значениями между двумя сетями. В состоянии синхронизации значения весовых коэффициентов одинаковы и могут использоваться как совместный ключ обеих сторон (A и B). Основная проблема заключается в том, что третья сторона (C, интруз) может попытаться также достичь состояния синхронизации (с двумя сетями A и B).

II. Расширение алгебры используемых чисел

Использование конструкции Кэли–Диксона (Cayley–Dickson) позволяет создавать расширения поля действительных чисел. Эта процедура дает возможность построить из действительных чисел последовательно их расширения: комплексные числа, кватернионы, октонионы, седенионы и т.д. Для криптографических применений разработаны модификации TPM с ис-

пользованием комплексных чисел (TPCM, Tree Parity Complex Machine), кватернионов (TPQM, TP Quaternion Machine) и октонионов (TPOM, TP Octonion Machine) [2–4]. Сама архитектура указанных сетей, как и идея их функционирования, схожи с TPM. Изменения касаются методов применения правила обучения и модификации функции знака, относящегося к выходному параметру сетей A и B. Так, например, для TPCM выходы нейронов – это четырехвалентные комплексные числа, принадлежащие множеству (1, 0), (0, 1), (-1, 0), (0, -1), а величины векторов весов – это комплексные числа, заключенные в квадрате $[-L,L]$ x $[-L, L]$.

Архитектура TPQM функционирует на основе кольца кватернионов. Правильное определение действий и изоморфизм с любым расширением тела действительных чисел, подтверждается теоремой Фробениуса. Кватернионы являются заключительным расширением тела действительных чисел, выполняющим условие ассоциативности операции умножения. Подтверждена эффективность использоваеия модели TPOM для вычисления хеш-функций [5].

В [6] проанализирована криптостойкость системы на основе TPM. Для защиты протокола при геометрической атаке, как минимум, необходимо значительное увеличение синаптической глубины, что также приводит к увеличению примерно на порядок времени, необходимого для наступления синхронизации. Таким образом, для обеспечения безопасности протокола при указанном способе атаки необходимы альтернативные способы защиты. Как показали исследования, проведенные авторами настоящего доклада (см. также [7]), имеется зависимость между наступлением процесса синхронизации сетей A и B и параметрами этих сетей. Ниже представлены новые результаты, касающиеся этого аспекта.

III. Моделирование и анализ процесса синхронизации ИНС

В нашем эксперименте две НС синхронизировали свои весовые коэффициенты обмениваясь выходными величинами на основе протокола TCP, причем пересылалась не явная информация, а хеш выходного значения на основе алгоритма SHA-512. Для сохранения результатов в разработанном приложении был использован EntityFraemwork и СУБД MS SQL Server. Весь процесс выполнялся с использованием авторского программного продукта, который позволял:

- выбирать конфигурацию сетей;
- подссчитывать количество проведенных опытов с данной конфигурацией;
- подсчитывать количество успешных опытов (сети синхронизированы);
- минимальное, максимальное и среднее количество итераций процесса синхронизации сетей;

Кроме того, мы получали отклонение полученных распределений от нормального распределения, а также индекс (метрика) Брея-Кертиса и расстояние по Хеллингеру. Для двух сетей с одинаковыми фиксированными параметрами проводилось не менее 1 тысячи опытов (попыток синхронизации). В таблице приведены некоторые результаты эксперимента. Здесь в четвертом стобце указано процентное отношение (u) числа синхронизаций к общему числу попыток синхронизации, в пятом столбце указано среднеквадратическое отклонение (СКО) и в шестом – индекс Брея-Кертиса (ИБК).

Таблица 1 – Результаты синхронизации весовых коэффициентов двух ИНС

Тип ИНС	K	N	$\pm L$	u	СКО	ИБК
TPCM	5	5	5	84,5	80,7	0,20
TPCM	6	7	6	92,9	68,6	0,17
TPQM	7	7	7	99,7	284,9	0,19
TPOM	7	7	7	99,6	2779	0,23

Установлено, что распределение количества синхронизировавшихся НС по числу операций (итераций) обучения близко к нормальному. В диапазон «трёх сигм» попадает 98.72 успешно синхронизировававшихся НС. Это можно использовать как параметр прерывания процесса синхронизации для снижения потенциальной возможности третьей стороны синхронизировать свои весовые коэффициенты с сетями A и B.

1. Kinzel, W. Interacting neural networks and cryptography / W. Kinzel, I. Kanter // Advances in Solid State Physics. – 2005. – Vol. 42. – P. 383–392.
2. Плонковски, М. Криптографическое преобразование информации на основе нейросетевых технологий / М. Плонковски, П. П. Урбанович // Труды БГТУ. Сер. VI. Физико-математические науки и информатика. – Минск: БГТУ. – 2005. – С. 161–164.
3. Plonkowski, M. The use of quaternions in the cryptographic key agreement protocol based on the architectures of the TPQM neural networks / M. Plonkowski, P. Urbanowicz, E. Lisitsa // Przegląd elektrotechniczny. – 2010. – Vol. 86, № 7. – P. 90–91.
4. Plonkowski, M. Split-complex numbers in neural cryptography / M. Plonkowski, P. Urbanowicz // Przegląd elektrotechniczny. – 2012. – Vol. 88, № 11b. – P. 340-341.
5. Urbanovich, P. The appearance of conflict when using the chaos function for calculating the hash code / P. Urbanovich, M. Plonkowski , K. Churikov // Przegląd elektrotechniczny. – 2012. – Vol. 88, № 11b. – P. 346-347.
6. Klimov, A. Analysis of Neural Cryptography / A. Klimov, A. Mityaguine, A. Shamir // Advances in Cryptology – ASIACRYPT 2002: 8th International Conference on the Theory and Application of Cryptology and Information Security Queenstown, New Zealand, December 1–5, 2002, Proceedings. P.288–298.
7. Урбанович, П. П. Моделирование и анализ процесса синхронизации нейронных сетей для обмена критической информацией / П. П. Урбанович, М. Долецки // Материалы XVII МНТК «Комплексная защита информации. Безопасность информационных технологий», 18.05.2012, Суздаль . – 2012. – С. 255-257.