функционально-полным набором для реализации технологии вычисления всех алгебраических функций по К. Шеннону.

Доказательство данной теоремы приведено в [3].

ЛИТЕРАТУРА

1 Крылов, С.М. Модели универсальных дискретно-аналоговых машин на основе машины Тьюринга / С.М. Крылов. // Электронное моделирование. - 1982. - № 3. - С.6-10.

2 Крылов, С.М. Функциональная полнота вычислительной системы. Компьютерные технологии в науке, практике и образовании / С.М. Крылов, М.В. Сараев. // Труды седьмой Всероссийской межвузовской научно-практической конференции. - Самара: СамГТУ, 2008.

3 Крылов, С.М. Синтез конфигурируемых блоков для аналого-цифровых систем-нА-кристалле с использованием гетерогенных функциональных компонентов / С.М. Крылов, М.В. Сараев. // Вестник Самарского государственного технического университета, Серия технические науки. - 2007. - № 2 (20).

УДК 681.3.006

П.П. Урбанович проф., д-р техн. наук;
М.Д. Планковски, К.В. Чуриков, магистрант
(БГТУ, г. Минск)

ЭФФЕКТИВНОСТЬ ГЕОМЕТРИЧЕСКОЙ АТАКИ НА КОМПЬЮТЕРНЫЕ СЕТИ

При современном развитии информационных технологий защита информации играет очень важную роль. Это связано главным образом, с очень динамичным развитием компьютерных сетей, в особенности сети Интернет. Безопасная пересылка данных является одним из важных вопросов в современном информационном мире. Поэтому существенную роль в этой сфере играет криптография, позволяющая шифровать важную информацию, защищая тем самым ее от несанкционированного доступа. В принципе вся современная криптография основана на теории чисел. Надежность криптографической системы зависит от трудности решения проблемы теории чисел. Однако с ростом вычислительной мощности современных компьютеров решение проблемы теории чисел занимает все меньше времени и системы становятся ненадежными. Поэтому так интересна новаторская идея криптографической системы на основе нейронных сетей.

Использование нейронных сетей для решения задач защиты информации впервые было предложено И. Кантер и В. Кинцель, и основывается на использовании известной сейчас архитектуры TPM (англ. Tree Parity Machine, древовидная машина четкости). При этом извест-

ные методы предполагают использование только целых действительных целых чисел как поля как поля для описания и анализа процессов в сети. Это является серьезным ограничением для дальнейшего совершенствования методов. В связи с этим актуальны исследования направленные на расширение поля используемых чисел в частности за счет комплексной плоскости.

Протокол обмена ключами, использующий нейронные сети, базируется на синхронном обучении сетей. Обучение двух нейронных сетей с использованием их общих выходных величин ведет к возникновению идентичных векторов весов. Сети обмениваются между собой выходными и входными значениями, при этом секретными остаются внутренние состояния весов векторов весов. Третья сторона (интруз), следящая за обменом информации между обеими сетями, не в состоянии восстановить внутреннее значение векторов весов ни одной из сетей. Следовательно, вектор весов может составлять секретный ключ, использующийся для дальнейшей передачи информации по незащищенным каналам.

Использование расширенного поля действительных чисел, а точнее протокола TPCM (Tree Parity Complex Machine, древовидная машина четкости на основе комплексных чисел) в виду своей специфики позволяет обеспечить более высокий уровень безопасности, чем классическая модель (TPM), основанная на арифметике действительных чисел.

Проведем компьютерный анализ безопасности процесса синхронизации нейронных сетей на основе протокола TPM и TPCM, используемых в криптографии.

Оценим возможность произведения геометрической атаки на архитектуру TPCM. Использование в реализации рассматриваемого типа атаки алгебры комплексных чисел накладывает необходимость изменения алгоритма геометрической атаки и его адаптации к специфике архитектуры TPCM.

Так как функция знака σ возвращает четыре величины, принадлежащие множеству $\{1, i, -1, -i\}$, то она делит плоскость на четыре части.

В этом алгоритме мы ищем вектор w_i, выходная величина которого будет близка не к 0, а к одной из линий деления плоскости. Вдобавок этот элемент не может быть выбран случайно. В случае геометрической атаки для архитектуры TPM было достаточно заменить выходную величину найденного вектора на противоположную по знаку. В случае архитектуры TPCM ситуация уже более сложная. А именно: модифицированная выходная величина вектора w_i не всегда ведет к

равенству $O^A=O^C$. Следовательно, нам надо ограничить область искомых внутренних векторов только теми, для которых изменение данной величины будет гарантировать равенство $O^A=O^C$.

Алгоритм геометрической атаки для архитектуры TPCM выглядит следующим образом:

1 Если архитектуры *A* и *B* имеют разные значения на выходах: $O^A \neq O^B$, то архитектура C, так же как *A* и *B* не производит активизацию внутреннего вектора весов.

2 Если *A* и *B* имеют равные выходы: $O^A = O^B$ и $O^A = O^C$, то оппонент C активизирует свой внутренний вектор весов в соответствии с выбранным правилом обучения.

3 Если *A* и *B* имеют одинаковые выходы: $O^A = O^B$, но $O^A \neq O^C$, тогда оппонент C находит вектор w_i, величина которого $||Re(ak)|-|Im(ak)||$ наименьшая (или близка к одной из линии деления плоскости). Область поиска мы ограничим только теми векторами, для которых изменение или перенесение величины в соседнюю четверть, гарантировано приведет к $O^A = O^C$. Этот процесс переноса обозначает умножение выходной величины на *i* или *-i* в зависимости от направления переноса найденной величины. Затем, благодаря этой операции, сеть C вместе с новой (исправленной) величиной активизирует свой внутренний вектор весов.

Таблица - Сравнение эффективности геометрической атаки в контексте безопасности архитектур TPM и TPCM

Архитектура	Время синхронизации сети *A* и *B*, измеряемое в количестве шагов	Время реализации геометрической атаки на сети *A и B*, измеряемое в количестве шагов
TPM	222,9	387,6
TPCM	2324,4	1000000(*)
Примечание - 1000000(*) - максимальное произведенное количество шагов, при котором оппонент C не смог синхронизироваться с наблюдаемыми сетями *A и B*.		

Как показали тесты (таблица), геометрическая атака очень опасна в процессе синхронизации сетей на основе архитектуры TPM. В то же время модель на основе TPCM характеризуется очень высокой степенью устойчивости к данным атакам. Даже значительное количество шагов (1.000.000) не ведет к синхронизации вектора весов сети интруза с сетями *A и B*.