УДК 004.032.26

ИССЛЕДОВАНИЕ ПОСТРОЕНИЯ КРИПТОГРАФИЧЕСКИХ СИСТЕМ НА ОСНОВЕ НЕЙРОННЫХ СЕТЕЙ

Автор: Грицкевич Т.В., магистрант каф.ПОИТ БГУИР

Научный руководитель: Ярмолик В. Н., д.т.н., профессор каф.ПОИТ БГУИР

Республика Беларусь, г.Минск, БГУИР, tplekhova@gmail.com

Реферат

Из-за роста вычислительных мощностей современных компьютеров, стала возможной дискредитация криптосистем еще недавно считавшихся почти нераскрываемыми. Т.о. возникает актуальность в поиске новых подходов к построению криптосистем. Пример подхода - построение криптосистем на основе нейронных сетей.

Доклад

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, всегда являлась важной задачей. В настоящее время использование криптографических методов в информационных системах стало особо актуальным.

С одной стороны, расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц.

С другой стороны, из-за процесса постоянного роста вычислительных мощностей современных компьютеров, а также технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически нераскрываемыми.

Таким образом, актуально искать новые подходы к решению данной задачи — например, нейросетевой подход — это одна из новых идей для построения криптографических систем. Разумеется, нейросетевым технологиям в их нынешнем состоянии не под силу создать что-либо, хоть отдаленно напоминающее по сложности человеческий мозг, однако уже очень многие его функции вполне поддаются моделированию, хотя и в весьма упрощенном варианте. В том числе и прямая передача информации от одной нейронной сети другой в процессе взаимного обучения.

В криптоанализе используется способность нейронных сетей исследовать пространство решений. Также имеется возможность создавать новые типы атак на существующие алгоритмы шифрования, основанные на том, что любая функции может быть представлена нейронной сетью. Взломав алгоритм, можно найти решение, по крайней мере, теоретически. При этом используются такие свойства нейронных сетей, как взаимное обучение, самообучение, и стохастическое поведение, а также низкая чувствительность к шуму, неточностям (искажения данных, весовых коэффициентов, ошибки в программе). Они позволяют решать проблемы криптографии с открытым ключом, распределения ключей, хеширования и генерации псевдослучайных чисел.

Для обмена ключами между двумя абонентами наиболее часто используется алгоритм Диффи-Хеллмана. Его более безопасная замена основана на синхронизации двух древовидных машин четности (TPM, tree parity machines). Синхронизация этих машин похожа на синхронизацию двух хаотических осцилляторов в теории хаотических связей (chaos communications).

Динамика двух сетей и их весовых коэффициентов нашла применение в явлении, где сети синхронизируют состояния с идентичными весовыми коэффициентами, зависящими от

времени. Эта концепция быстрой синхронизации по взаимному обучению может быть применена к протоколу обмена секретным ключом через публичный канал. А сгенерированный ключ может быть использован для шифрования и дешифрования передаваемого сообщения. Алгоритм не оперирует большими числами и методами из теории чисел, следовательно, приводит к быстрой синхронизации открытого ключа. Безопасность нейрокриптографии в процессе обсуждения,ведт из-за того, что метод основан на стохастическом процессе, есть небольшой шанс, что злоумышленник синхронизируется с ключом.

Также, было установлено, что защищенность обычных криптографических систем можно улучшить, увеличив длину ключа. В нейрокриптографии вместо ключа увеличивается синаптическая длина L. Это увеличивает сложность атаки экспоненциально, в то время как затраты абонентов на дешифрацию растут полиномиально. Таким образом, взлом подобной системы является NP-сложной задачей.

Есть утверждения, что исходный алгоритм нейросинхронизации может быть сломан, по крайней мере, тремя видами атак: геометрической, вероятностным анализом и генетическими алгоритмами. Хотя данная реализация небезопасна, идеи случайной синхронизации могут привести к абсолютно безопасной схеме.

Например, можно значетельно улучшить защищенность обычных криптографических систем, увеличив длину ключа. В нейросетевом подходе вместо ключа увеличивается синаптическая длина L. Это увеличивает сложность атаки экспоненциально, в то время как затраты абонентов на дешифрацию растут полиномиально. Таким образом, взлом подобной системы является NP-сложной задачей.

Одна из идей построения криптографической системы на основе нейронных сетей - это система на базе взаимодействующих нейронных сетей, представленная Кантером, Кинзело и Кантером (ККК), использующая множество циклов, в которых каждая сторона выявляет один бит информации о текущем состоянии, а затем модифицирует его в соответствии с информацией, полученной от другой стороны. Если обозначить последовательность двух сторон, как A_i и B_i, то расстояние (A_{i+1},B_{i+1}) меньше расстояния (A_i,B_i) и $A_i = B_i$ для всех $i > i_0$. С точки зрения криптоанализа, состояния сторон становятся быстродвижущимися целями, а его общая задача состоит в том, как объединить биты информации о двух сходящихся последовательностях неизвестных состояний [3].

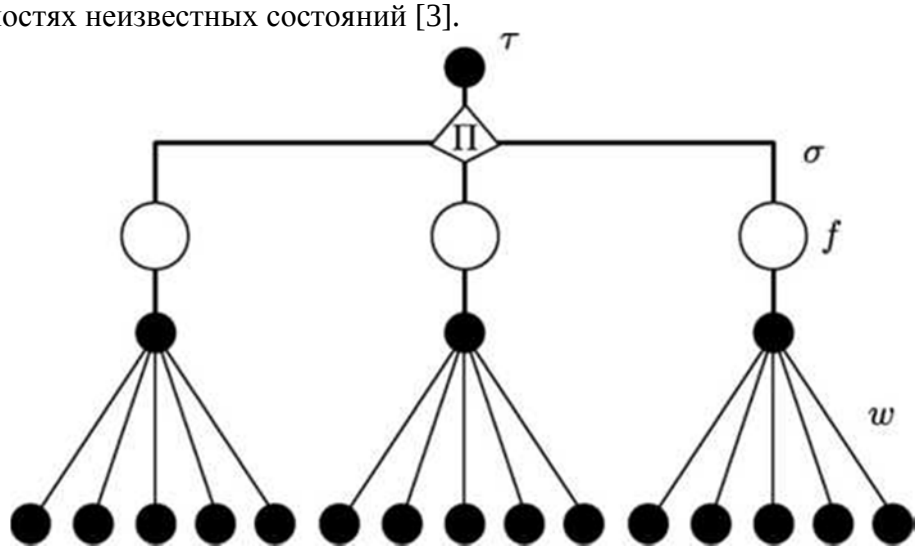

Рисунок 1 – Параллельная машина для *K* — 3 с хаотичным отображением

В проблеме совместного обучения каждая сеть используется и как обучающая сторона, и как сторона обучающаяся, и не существует фиксированной цели, к которой необходимо стремится. Наоборот, они преследуют друг друга по хаотичной траектории, которая первоначально управляется общей последовательностью случайных входов.

Каждая сторона в предложенной ККК-конструкции использует двухслойную нейронную сеть. Первый слой содержит K независимых персептронов, в то время как второй слой вычисляет равенство K скрытых слоев. Каждый из K персептронов имеет N весов $w_{k,n}$ (где $1 \le k \le K$ и $1 \le n \le N$). Эти веса целые числа в области {L, …, -L}, которые могут изменяться во времени. Дано N битовых входных значений ($x_{k,1}$, …, $x_{k,N}$) (где $x_{k,n} \in$ {-1, +1}), персептрон возвращает знак (который также принадлежит {-*l*, +*l*}) произведения $= \sum_{=1}$, . Выход o_k персептрона имеет простое геометрическое толкование: геперплоскость, которая перпендикулярна вектору весовых коэффициентов w, делит пространство пополам, а выход персептрона для входа x показывает, находятся x и w по одну сторону гиперплоскости или нет (т.е. меньше или больше 90° угол между w и x). Выход нейронной сети определяется как равенство $= \prod_{=1}$ выходов K персептронов.

В схеме ККК две стороны A и B начинают с произвольных некоррелированных матриц весовых коэффициентов { , }. В каждом цикле новая произвольная матрица входов { , } открыто выбирается (например, используя генератор псевдослучайной последовательности бит), а каждая сторона объявляет выход своей своей нейронной сети на заданном общем входном сигнале. Если два выходных бита совпадают, стороны остаются без действия и проходят в следующий цикл; иначе каждая сторона обучает собственную нейронную сеть в соответствии с выходом другой стороны. При обучении используется классическое правило обучения Хебба для обновления весовых коэффициентов персептрона. Тем не менее, каждой стороне известно только равенство выходов персептронов других сторон и таким образом правило модифицируется: в методе ККК каждая сторона модифицирует только те персептроны в своей сети, чьи скрытые входы отличаются от обозначенного выхода. С этой поправкой ККК показывает, что для некоторых вариантов K, N, L матрицы весовых коэффициентов двух сторон становятся непараллельными (то есть , = − ,), для всех k и n) после достаточного небольшого числа циклов, и с этого момента они всегда формируют негативные выходы и обновляют свои весовые коэфициенты, переходя в новые непараллельные состояния. Две стороны могут быть осведомленными о полученной синхронизации, отмечая, что их выходные значения совпадают в течении 20-30 последовательных шагов. Раз в их сети стали синхронизированными, две стороны могли остановить и вычислить общий криптографический ключ путем хеширования своей текущей матрицы весовых коэффициентов (или ее отрицания).

Для того, чтобы показать возможность применения криптографических систем на основе нейронных сетей был проведен ряд экспериментов. Задачей экспериментов было показать, возможность использования подхода реализации криптографических систем на основе нейронных сетей, достигнуть сравнительно быстрого времени синхронизации нейронных сетей. Эксперименты производились над разными типами нейронных сетей: Tree Parity Machines, нейронные сети с хаотичным отображением, нейронные сети с обратной связью.

N	Среднее количество сообщений, шт	Среднее затраченное время CPU, с
3	798,53	0,134
4	370,63	0,072
5	362, 23	0,083

8	339,67	0,111
16	365,74	0,212
32	430,96	0,476
64	483,31	1,050
128	557,04	2,670
256	589,64	6,036
512	659,72	11,165
1024	720,32	24,436

Таблица 1 - Среднее количество сообщений при синхронизации TPM и среднее затраченное время CPU в зависимости от коэффициента N, определяющего количество входных нейронов

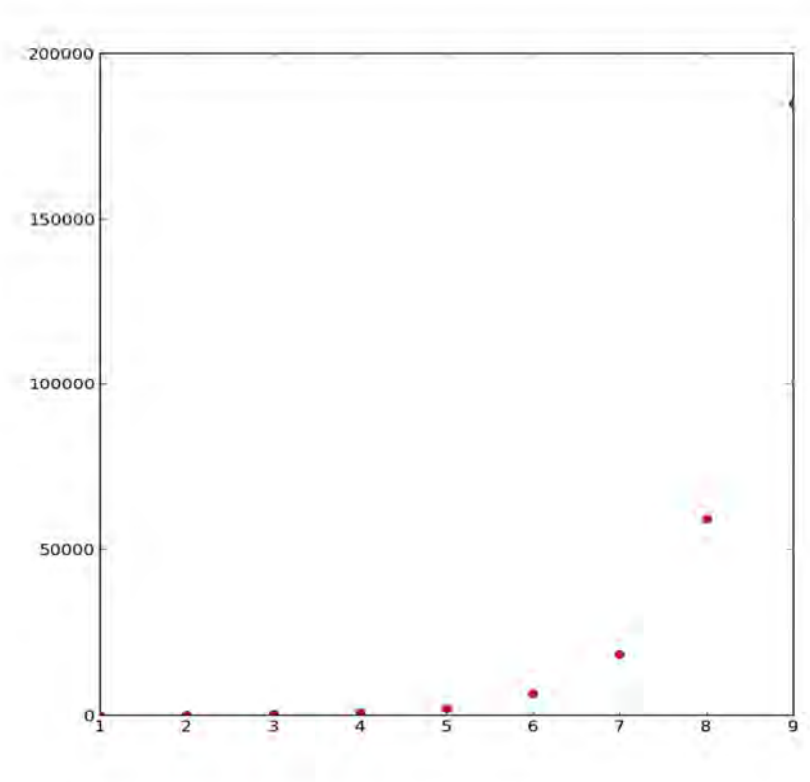

Рисунок 2 - График зависимости среднего количества сообщений от L при конфигурации сети TPM K=4, N=4

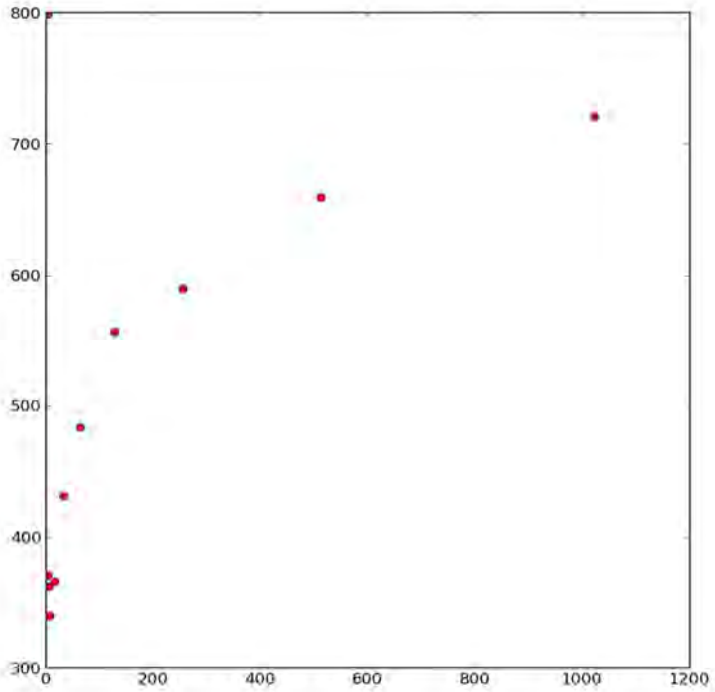

Рисунок 3 - График зависимости среднего количества сообщений от N при конфигурации сети TPM K=4, L=3

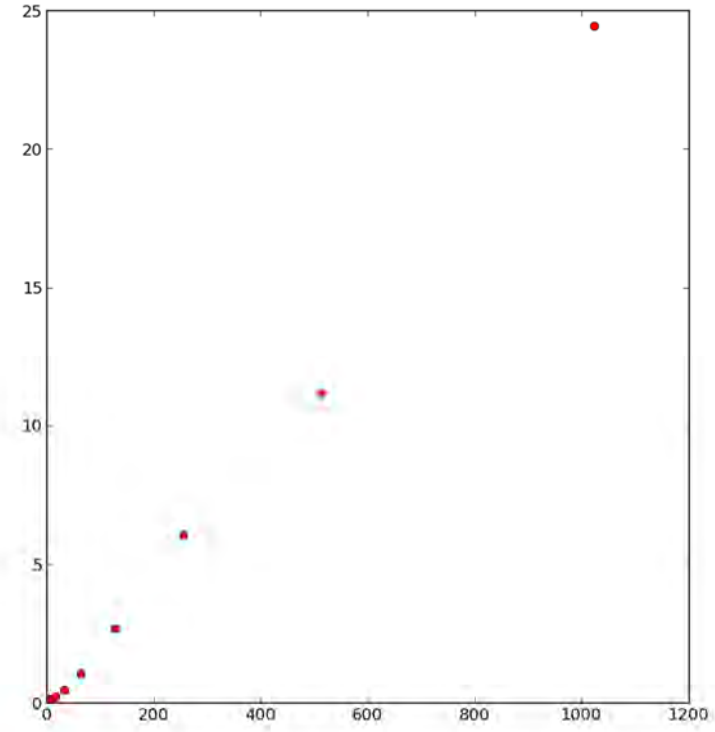

Рисунок 4 - График зависимости среднего времени CPU от N при конфигурации сети TPM K=4, L=3

Для каждого вида нейронной сети было найдено оптимальное соотношение между сложностью полученной системы и времени, потраченном на ее синхронизацию. Для

приведенного примера TPM при конфигурации K=4, L=3 наиболее оптимальное соотношение достигалось при N от 256 до 512.

Список использованных источников:

[1] Dourlens, S., The first definition of the Neuro-Cryptography (AI Neural-Cryptography) applied to DES cryptanalysis by Sebastien Dourlens – 1995, France.

[2] Kinzel, W., Neural Cryptography — Description of one kind of neural cryptography at the University of Würzburg – 2005, Germany.

[3] Червяков, Н.И., Применение искусственных нейронных сетей и системы остаточных классов в криптографии / Червяков Н.И., Евдокимов А.А., Галушкин А.И., Лавриненко И.Н. / М.: ФИЗМАТЛИТ, 2012.- 280 с.