МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №16 НА ТЕМУ:**

**Согласование криптографических ключей на основе технологий искусственных нейросетей**

Выполнила студентка 3 курса 4 группы

Сятковская Екатерина

Минск 2023

**Цель:** Изучение основ построения и функционирования искусственных нейронных сетей (ИНС), а также использования ИНС в криптографии; приобретение практических навыков программной реализации алгоритма согласования ключевой информации на основе технологии ИНС.

**Теоретические сведения**

**Нейронная сеть** – математическая модель, построенная по принципу организации и функционирования биологических нейронных сетей. Искусственные нейронные сети (ИНС) состоят из **перцептронов**, являющихся аналогами биологических нейронов. На рисунке 1.1 представлена схема перцептрона.

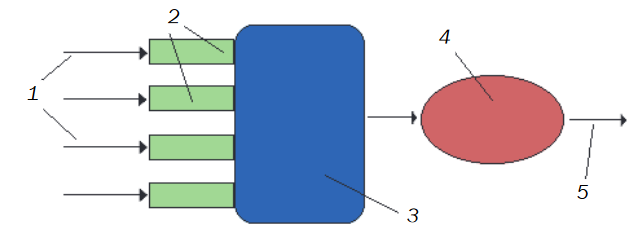


Рисунок 1.1 – Схема искусственного нейрона (перцептрона)

1 – Входы перцептрона;

2 – Веса;

3 – Суммирующий блок;

4 – Блок активации;

5 – Выход.

На входы перцептрона поступают сигналы (могут передаваться и от других перцептронов), каждый их которых умножается на свой вес. Далее взвешенные сигналы поступают в суммирующий блок, который аггрегирует все сигналы во взвешенную сумму. Взвешенная сумма пропускается через блок активации, которые на её основе вычисляет выходной сигнал.

**Древовидная машина чётности (Tree Parity Machine, TPM)** – многослойная искусственная нейронная сеть, состоящая из одного выходного нейрона, *K* скрытых нейронов и *K\*N* входных нейронов. Схема TPM представлена на рисунке 1.2.

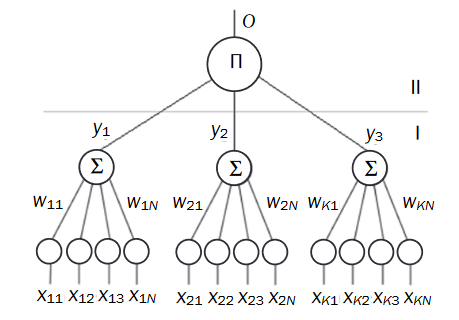


Рисунок 1.2 – Схема TPM

На входные нейроны подаются сигналы, которые суммируются скрытыми нейронами. Сигналы с выходов скрытых нейронов суммируются выходным нейроном.

Синхронизация двух TPM-машин может использоваться для обмена ключевой информацией, аналогично обмену ключами в алгоритме Диффи-Хеллмана.

Алгоритм синхронизации двух TPM-машин:

1. Сгенерировать для каждой машины вектор случайных весовых коэффициентов;

2. Сгенерировать случайных вектор из *K\*N* входных значений;

3. Вычислить значения на выходах скрытых нейронов;

4. Вычислить значения на выходах выходных нейронов;

5. Если выходные значения не равны, применить правило обучения для обеих машин: машины обучаются на основе выходных значений друг друга;

6. Если вектора входных весов у двух TPM-машин равны, они достигли синхронизации. Иначе, перейти к шагу 2.

**Правило обучения Хебба** – правило для синхронизации TPM-машин, которое может быть сформулировано следующим образом: если нейрон получает входной сигнал другого нейрона и выходные значения обоих нейронов имеют одинаковый знак, веса входных значений должны быть увеличены. Математически правило описывается следующим образом:

Где *Δwi* – приращение веса входного параметра;

*σi* – знак взвешенного входного параметра нейрона, либо 0;

*xi* – значение входного параметра;

Θ – функция, значение которой равно 1, если входные параметры равны, иначе значение функции равно 0;

*τ1* – значение выходного параметра синхронизируемого нейрона;

*τ1* – значение выходного параметра второго нейрона.

**Практическая часть**

Разработанное приложение производит 500 синхронизаций двух TPM-машин с заданными параметрами и применением правила обучения Хебба. Приложение также при каждой синхронизации подсчитывает число шагов, за которое она происходит, и среднее значение шагов для синхронизации на данном шаге. Затем на основе полученных значений строится график зависимости среднего числа шагов, необходимых для полной синхронизации двух машин.

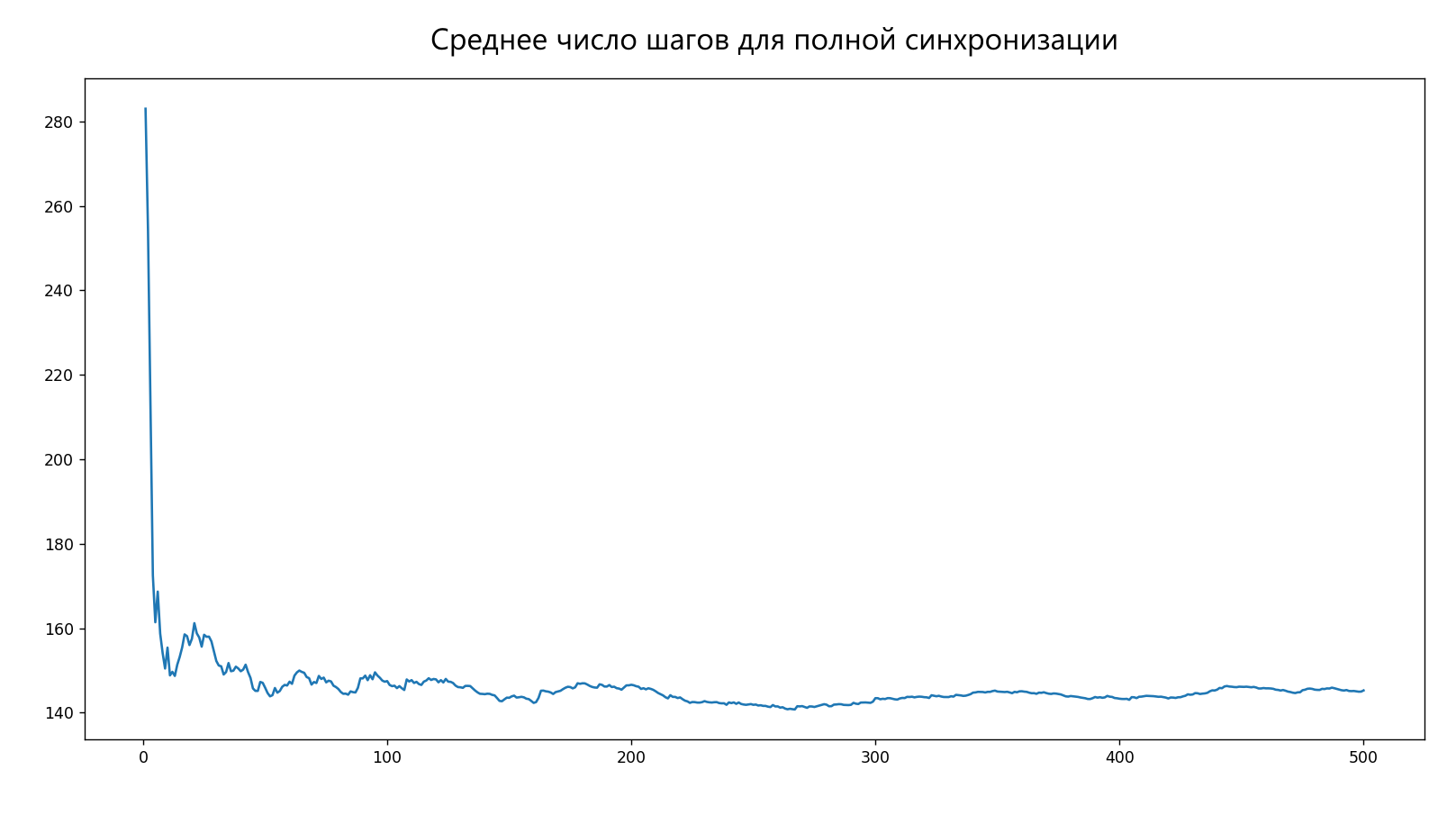


Рисунок 2.1 – График зависимости среднего числа шагов для полной синхронизации от числа синхронизаций

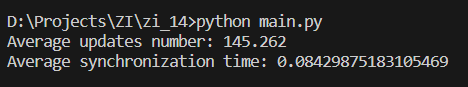
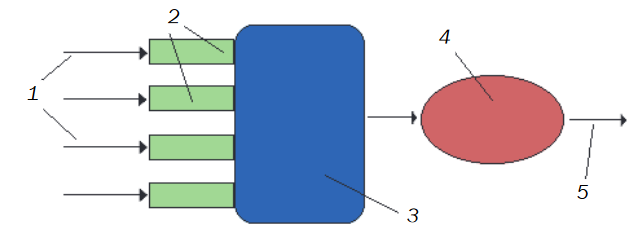


Рисунок 2.2 – Консольный вывод приложения

**Вывод:** В ходе лабораторной работы было разработано приложение, позволяющее синхронизировать 2 TPM-машины. Среднее число шагов для полной синхронизации для заданных параметров – 145. Среднее время полной синхронизации двух машин составило примерно 0.084 секунды.

**Контрольные вопросы**

**1. Изобразить схематично структуру персептрона и пояснить аналогии между его компонентами и частями биологического нейрона.**



1 – Входы перцептрона (дендриты);

2 – Веса (синапсы);

3 – Суммирующий блок (ядро);

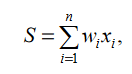
4 – Блок активации (основание аксона);

5 – Выход (аксон).

**2. Охарактеризовать (и показать на примерах) области использования ИНС.**

ИНС активно используются при анализе и обработке больших массивов информации (задачи классификации и прогнозирования) и при обучении искусственного интеллекта. Некоторые методы на основе ИНС могут быть использованы в криптографии для согласования ключевой информации.

**3. Как в простейшем виде записывается формальное представление персептрона?**



Где S – выходной сигнал;

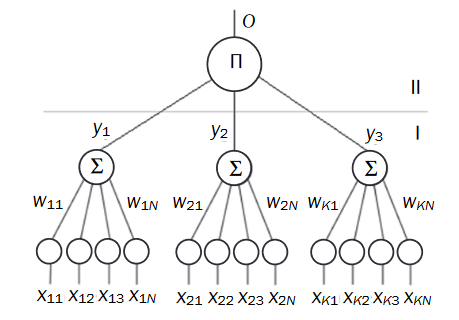
wi – вес входного сигнала;

xi – значение входного сигнала.

**4. Охарактеризовать (и показать на примерах) области использования ИНС в криптографии.**

Некоторые методы на основе ИНС могут быть использованы в криптографии для согласования ключевой информации. Примером может выступать метод на основе синхронизации TPM-машин.

**5. Дать пояснение к структуре и функционалу информационной системы на основе ИНС, предназначенной для согласования ключевой информации.**



На входные нейроны подаются сигналы, которые суммируются скрытыми нейронами. Сигналы с выходов скрытых нейронов суммируются выходным нейроном.

**6. Дать характеристику известным алгоритмам обучения ИНС.**

Все алгоритмы обучения ИНС можно разделить на методы обучения с учителем и без учителя. Обучение без учителя предусматривает наличие только входных данных (такие методы могут решать задачи кластеризации или масштабирования входных данных).

**7. Какие алгоритмы используются для обучения ИНС, предназначенных для согласования ключевой информации между двумя сторонами?**

**Правило обучения Хебба** – правило для синхронизации TPM-машин, которое может быть сформулировано следующим образом: если нейрон получает входной сигнал другого нейрона и выходные значения обоих нейронов имеют одинаковый знак, веса входных значений должны быть увеличены.

**Правило Анти-Хебба** – если нейрон получает входной сигнал другого нейрона и выходные значения обоих нейронов имеют одинаковый знак, веса входных значений должны быть уменьшены.

**Обучение на основе случайного блуждания** – строится на запоминании и забывании значений из определённого диапазона с корректировками на каждом шаге в зависимости от степени синхронизации.

**8. Могут ли легитимно участвовать в процессе синхронизации более трех сетей? Мотивируйте ответ.**

Да. Если эти сети выступают в качестве посредников передачи информации, можно создать цепочку из TPM-машин, которые на каждом шаге будут синхронизироваться между собой. Однако подобный способ является крайне ресурсоёмким по вычислительной мощности.

**9. Дать характеристику криптостойкости системы на основе двух взаимодействующих ИНС.**

Так как при синхронизации используются случайные вектора входных значений, системы обладает высокой криптостойкостью, однако она должна быть достаточно быстрой, чтобы при потенциальная атакующая нейронная сеть не успела синхронизироваться с одной из машин. При равных вычислительных мощностях атакующая нейросеть никогда не будет успевать синхронизироватся, так как ей, как правило, не известны сгенерированные случайные значения входных параметров.

**10. Какие виды атак на нейрокриптографические системы вам известны? В чем заключается их сущность?**

**Брутфорс** – атакующий должен проверить все возможные варианты весов.

**Обучение собственной TPM** – атакующий имеет такую же TPM, которые есть в атакуемой системе, и пытается синхронизировать её с системными машинами. Для подобных атак нужны большие вычислительные мощности, так как атакующая TPM обучается медленнее, чем синхронизируются системные машины.