Применение взаимодействующих нейронных сетей в криптографии

Ходаков Дмитрий.

March 14, 2014

1. Постановка задачи
   - Передача ключей
   - Tree Parity Machines

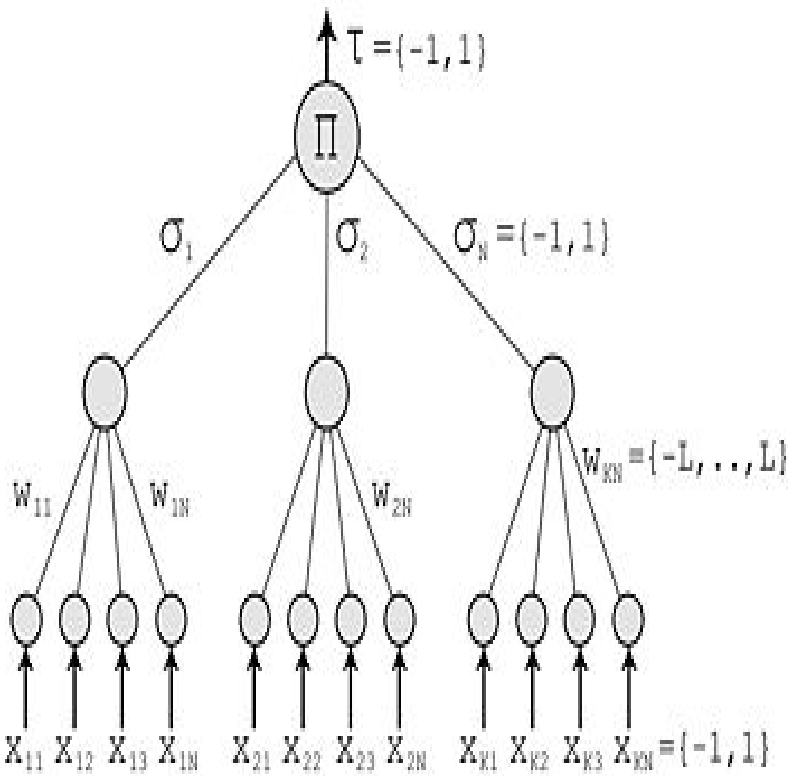
2. Результаты
   - Зависимость скорости сходимости от eta
   - Зависимость скорости сходимости от L
   - Теоретическая формула для скорости обучения

Передача ключей

- Безопасная замена алгоритма Диффи-Хеллмана
- Основана на синхронизации двух нейросетей
- Они называются древовидных машин четности (TPM, tree parity machines)

Tree Parity Machines

- Многоуровневая нейронная сети прямого распространения
- Входные нейроны принимают значения -1, +1
- Веса между скрытыми нейронами принимают значения [-L, +L]
- Значения скрытого нейрона ч= сигн w*x
- Значения выходного нейрона т = ...



Tree Parity Machines - алгоритм

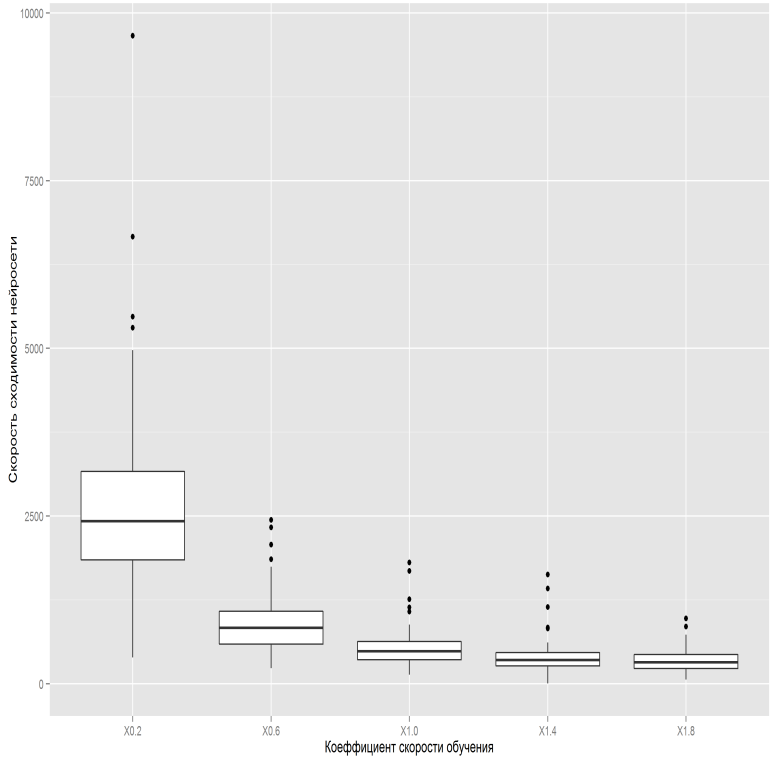
У каждого абонента (А или Б) есть своя TPM. Синхронизация:

- Задаём случайные значения весовых коэффициентов
- Выполняем следующие шаги, пока не наступит синхронизация
- Генерируем случайный входной вектор X
- Вычисляем значения скрытых нейронов
- Вычисляем значение выходного нейрона
- Сравниваем выходы двух TPM:
- Выходы разные: переход к п.2.1
- Выходы одинаковые: применяем выбранное правило к весовым коэффициентам

Для обновления весовых коэффициентов могут использоваться следующие правила:
Правило Хебба: $w_i^+ = w_i + \sigma_i x_i \Theta(\sigma_i \tau)\Theta(\tau^A \tau^B)$

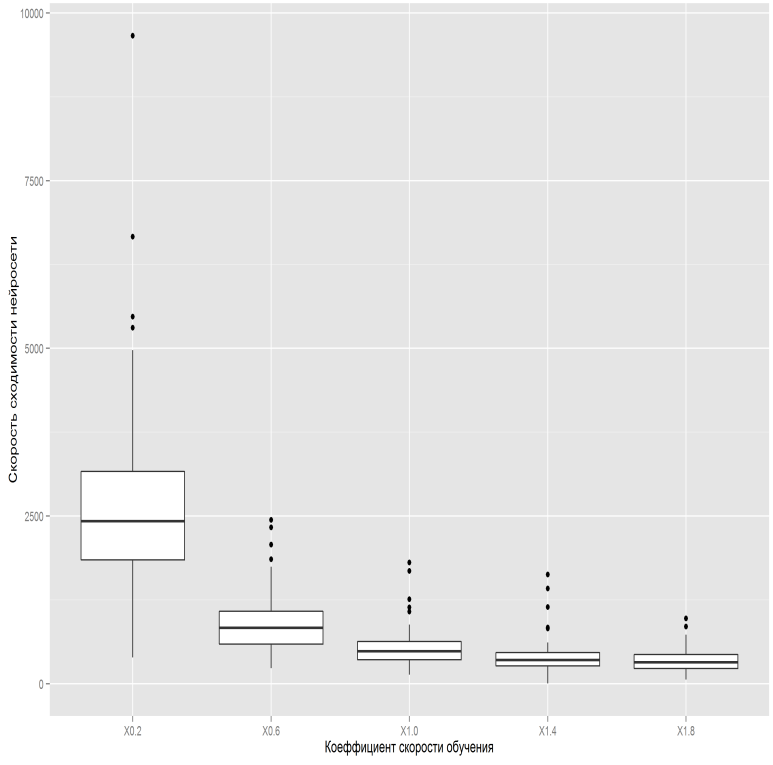
Зависимость скорости сходимости от L

Посмотрим, какова скорость схождения сети в зависимости от константы обучения.



Зависимость скорости сходимости от L

Посмотрим, какова скорость схождения сети в зависимости от константы обучения.



Теоретическая формула для скорости обучения

Посмотрим, какова скорость схождения сети в зависимости от константы обучения.