dr hab. inż. Franciszek Seredyński
Polsko-Japońska Wyższa Szkoła Technik Komputerowych
oraz
Instytut Podstaw Informatyki PAN

Warszawa, 28.06.2008

Recenzja

rozprawy doktorskiej mgr Piotra Kotlarza nt.

Sieci neuronowe we wspomaganiu rozwiązywania problemów kryptologii

1. Problematyka naukowa oraz przedmiot rozprawy

Recenzowana praca doktorska poświęcona jest problemom kryptografii, a w szczególności jej celem jest opracowanie i zbadanie możliwości zastosowania jednego z narzędzi sztucznej inteligencji, jakim są sieci neuronowe do tworzenia algorytmów kryptograficznych.

W dobie zaawansowanych technologii teleinformatycznych oraz szybko rozwijających się usług typu e-bankowość, e-urząd, itp. kryptografia, niegdyś rozwijana w sposób dyskretny, stała się jedną z czołowych i głośnych dziedzin informatyki. Szybki rozwój mocy obliczeniowych współczesnych komputerów jest ciagłym wyzwaniem dla istniejących i tworzonych standardów kryptograficznych. Rozszerzył się również znacznie wachlarz zastosowań kryptografii i wymogów co do algorytmów kryptograficznych. Dziś kryptografia jest stosowana nie tylko do szyfrowania bardzo ważnych informacji i danych (duże wymagania kryptograficzne), ale również do szyfrownia np. bieżących rozmów telefonicznych w sieciach komórkowych, czy też do szyfrowania danych technicznych przesyłanych między współpracujacymi urzadzeniami (umiarkowane wymagania kryptograficzne). Z tych właśnie powodów, pomimo istnienia klasycznych narzędzi kryptograficznych wykorzystujących określone działy matematyki, poszukuje się dzisiaj nowych perspektywicznych narzędzi i algorytmów kryptograficznych.

Praca doktorska mgr Kotlarza wpisuje się dobrze w ten nurt poszukiwań nowych metod i narzędzi kryptograficznych. W swojej pracy skupia sie on na eksploracji możliwości stosowania dla celów kryptograficznych narzędzia jakim są sieci neuronowe, a w szczególności tej cechy sieci neuronowych jaką jest tzw. uczenie z nauczycielem.

Pierwowzorem kryptograficznym w rozważaniach podejmowanych w pracy jest powszechnie znany standard kryptograficzny DES. Doktorant wyróżnia w nim dwa, podstawowe z punktu widzenia pracy DES-a, elementy koncepcyjne, a mianowicie element realizujący permutacje oraz element realizujący nieliniowe przekształcenia, znany jako S-Blok. Następnie, wykorzystując proces uczenia się realizuje neuronowe odpowiedniki tych elementów. Te neuronowe elementy wykorzystuje później do stworzenia koncepcji neuronowego układu szyfrujacego i wskazuje możliwości zastosowania takiego układu. W ten sposób osiąga cel stawiany sobie w pracy, potwierdzając tezę o możliwości realizacji systemu kryptograficznego z użyciem sieci neuronowych.