



POLSKO-JAPONSKA WYŻSZA SZKOŁA TECHNIK KOMPUTEROWYCH

Warszawa, 9 sierpnia 2008 r.

prof. dr hab. Witold Kosiński
Polsko-Japońska Wyższa Szkoła
Technik Komputerowych, Warszawa
Uniwersytet Kazimierza Wielkiego
Bydgoszcz

Opinia na temat rozprawy doktorskiej mgra Piotra Kotlarza :

Sieci neuronowe we wspomaganiu rozwiązywania problemów
kryptologii

Niniejszą recenzję przygotowałem na zlecenie Rady Naukowej Instytutu Podstawowych Problemów Techniki PAN, która prowadzi przewód doktorski mgra Piotra Kotlarza. Promotorem rozprawy jest doc. dr habil. inż. Zbigniew Kotulski.

Uwagi wstępne

Koniec ubiegłego wieku i początek obecnego to czas, kiedy kryptologia stała się dostępną i powszechną dyscypliną naukową. Powstaje wiele publikacji na temat kryptografii, dokonuje się rozstrzygnięć kolejnego konkursu na nowy standard szyfrowania, w Polsce oraz na świecie organizowane są konferencje naukowe tematycznie związane z bezpieczeństwem informacji.

Szyfrowanie jest sposobem ochrony informacji przed zinterpretowaniem ich przez osoby niepowołane. Jednocześnie jest to jedyny znany i skuteczny sposób realizacji ochrony informacji przesyłanej w sieci, kanałami otwartymi. W szyfrowaniu informacji wykorzystuje się szyfry - tj. rodzinę przekształceń służących do nadawania informacji postaci niezrozumiałej lub bezużytecznej dla napastnika. Z szyfrowaniem związane są takie pojęcia jak: nauka o szyfrach, nauka o konstruowaniu i stosowaniu szyfrów, zwana kryptografią i kryptoanaliza - nauka o łamaniu szyfrów. Sam proces szyfrowania polega na przekształceniu za pomocą funkcji oraz hasła szyfrowania (tzw. klucza) informacji jawnej w inną zwaną kryptogram lub tekst zaszyfrowany. Proces odwrotny, nazywany deszyfrowaniem polega na tym, że kryptogram jest przekształcany z powrotem w oryginalną informację jawną za pomocą pewnej funkcji matematycznej i klucza.

Przedstawiona do recenzji rozprawa doktorska choć odnosi się do wszystkie wymienionych działów zajmuje się głównie konstrukcją sieci neuronowej, która byłaby w stanie zrealizować różne algorytmy szyfrujące.

Sieci neuronowe należą do podstawowych narzędzi inteligencji obliczeniowej, znanej dotąd pod nazwą sztucznej inteligencji.

Skoro wspomina się sztuczną inteligencję to pojawia się bezpośrednio skojarzenie do jej wykorzystania w kryptoanalizie, łamaniu szyfrów czy wydobycie z szyfrogramów tekstów oryginalnych, ukrytych.

Autor niniejszej rozprawy nie poszedł w tym kierunku. Zaproponował coś innego.

Zawartość rozprawy

Rozprawa składa się z 10 rozdziałów, bibliografii, która zawiera 75 pozycji, spisów rysunków i tablic. Praca liczy 116 stron.

Rozdział 1 zawiera cel i zakres pracy, motywacje do podjęcia tematyki badawczej, będącej przedmiotem rozprawy. Tutaj też została sformułowana teza. Rozdział 2 to wprowadzenie podstaw teoretycznych z zakresu kryptologii, dotyczących wyników badań przedstawionych w tej pracy.

W rozdziale 3 wprowadzono zagadnienia z zakresu podstaw matematycznych dla permutacji oraz S -bloków. Została poruszona tematyka projektowania szyfrów. Opisano także wybrane zagadnienia z dziedziny sieci neuronowych.

Rozdział 4 zawiera przegląd metod implementacji szyfrów, począwszy od historycznych do współczesnych implementacji programowych i sprzętowych. W rozdziale 5 umieszczono przegląd obszarów kryptologii, w których wykorzystywane są sieci neuronowe.

Rozdział 6 zawiera główne, oryginalne, wyniki autora w zakresie realizacji elementarnych przekształceń szyfrujących, wykorzystującej techniki znane z teorii sztucznych sieci neuronowych.

Rozdział 7 stanowi ważne uzupełnienie wyników z rozdziału poprzedniego. Umieszczono w nim propozycje realizacji szyfru blokowego opartego na modelu sieci S-P, za pomocą neuronowych układów realizujących funkcję S -blok oraz permutacje.

W Rozdziale 8 przedstawiono propozycje możliwych rozwiązań w zakresie konstrukcji protokołu kryptograficznego, umożliwiającego wykorzystanie neuronowego układu szyfrującego w rozwiązaniach, opartych na architekturze klient-serwer. Rozdział 9 zawiera opis możliwości wykorzystania neuronowych realizacji funkcji S -blok oraz permutacji do realizacji szyfrów.

Podsumowanie prowadzonych rozważań w całej pracy oraz przedstawienie obszarów, w których badania będą kontynuowane w przyszłości, składają się na Rozdział 10.

