POLSKO-JAPOŃSKA WYŻSZA SZKOŁA TECHNIK KOMPUTEROWYCH

ポーランド日本情報工科大学

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 kryptolgii

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 sie rozstrzygnięć kolejnego konkursu na nowy standard szyfrowania, w Polsce oraz na świecie organizowane są konferencję 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 wymieninych działów zajmuje sie głownie konstrukcją siecii neuronowej, która byłaby w stanie zrealizowac różne algorytmy szyfrujące.

ul. Koszykowa 86, 02-008 Warszawa; tel: (0-22) 58-44-500; fax: (0-22) 58-44-501;
e-mail: pjwstk@pjwstk.edu.pl; www.pjwstk.edu.pl