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

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

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

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

Zawartość rozprawy

Rozprawa skład się z 10 rozdziałów, bibliografi, 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.

Ocena wyników rozprawy

Metody z zakresu kryptologii, z natury dość złożone, zostały przez mgra Piotra Kotlarza należycie przedstawione. Zamieszczone przykłady są dość przejrzyste. Podobnie rzecz ma się ze sposobem prezentacji.

W celu wykazania tezy pracy doktorant przeprowadza dość dokładną analizę istniejącej literatury i obserwowanych przy okazji konferencji i ogłaszanych konkursów szyfrograficznych trendów rozwojowych współczesnej kryptologii. Przedstawia też analizę aktualnego stanu badań światowych w zakresie możliwości zastosowania sieci neuronowych w kryptologii. Następnie formułuje koncepcję wykorzystania sieci neuronowych do budowy szyfrów blokowych. To jest główny wynik pracy, który obok teoretycznego wyprowadzenia struktury budowanych modułów wielowarstwowej sieci komputerowej typu S-P, jest wzbogacony o własne oprogramowanie, umożliwiające prowadzenie badań eksperymentalnych dotyczących budowy neuronowego układu szyfrującego. Rezultatem tych prac jest konstrukcja sieci neuronowych zdolnych do realizacji przekształceń liniowych, a także nieliniowych, wykorzystywanych przez szyfry symetryczne. Autor nie ogranicza sie tylko do tego. W dalszej części rozprawy (Rozdziały 7, 8 i 9) wskazuje dodatkowe możliwości, jakie powstają dzięki neuronowej implementacji szyfrów blokowych, wykorzystanie sieci jako elementu klucza, a także do generowania klucza cyklu.

Pierwszych wrażeń przynosi cześć wstępna, w której autor może zbyt skromnie traktuje podstawy matematyczne szyfrowania. Popełnia przy tym liczne błędy w oznaczeniach, str.15, 17, 19, 25, 61, 67. i nazewnictwie (str. 30). Brakuje też podstawowych definicji pojęć występujących w kryteriach projektowych, np. brak definicji zrównoważenia.

Jeśli chodzi o język, to doktorant nagminnie stosuje inwersję, tzn. w miejsce: *Napierw zostanie przedstawiona..* autor pisze : *Najpierw przedstawiona będzie..* (str.89). Styl taki - tak często wstosowany w gazetach - nie powinien być naśladowany w rozprawach naukowych. Użycie od czasu do czasu inwersji jest dopuszczalne, ale to co robi doktorant w końcowej części rozprawy (np. str.66, 89, 91, 94, 96, 98 itd.), jest naganne. W wielu miejscach w zdaniach brakuje przecinków, co utrudnia czytanie rozprawy. Niestety w kilku miejscach autor nie ustrzegł się użycia błędnej frazy: *W oparciu o ...*, gdzie w miejsce kropek nie stała ściana (np. str.14 i 48).

W części prezentującej autorski pomysł doktoranta wykorzystania sieci neuronowych do implementacji funkcji kryptograficznych pojawiają się rysunki. Wagi są na nich oznaczane tą samą literą w i jednym indeksem bieżącym, bez względu na warstwę, w jakiej występuje. Dla mniej wtajemniczonych, a przywykłych do oznaczeń z książek poświęconych sieciom neu-

ronowym, takie postępowanie nie jest dopuszczalne. Pojawienie się następnej warstwy wymusza w nich dopisanie dodatkowego wskaźnika, a nawet dwóch: jednego odpowiedzialnego za numer warstwy (pisanego zazwyczaj na górze) i drugiego – wskazującego numer neuronu, z którym bieżący neuron (o tej wadze) jest połączony. Mogę zrozumieć oszczedność autora w pisaniu wskaźników. Wypadałoby jednak przygotować czytelnika do tego skrótu w oznaczeniach małą uwagą porządkową. Dla recenzenta cześć rysunków Roz. 6 utrudnia śledzenie prezentacji autora.

Dyskusyjne wydaje się przyjęcie, że każdy neuron ma zawsze (i tylko) dwa wejścia. Może warto byłoby tę kwestię poruszyć w trakcie obrony.

Rozprawa dowodzi dużej pomysłowości i biegłego opanowania programowania przez doktoranta. Realizacja sieciowa podstawowych funkcji kryptograficznych: przestawiena (permutacji) i podstawiena (S-bloku) , to duże osiągnięcie autora. W szczególności początkowa drażniąca recenzenta złożoność (powiedzmy więcej - kaskadowość) budowanej sieci (por .p. 6.3.1) okazuje się bardzo trafna, gdyż zmiana realizowanego S-bloku jest dokonywana w bardzo szybki i wygodny sposób, bez konieczności zmiany struktury sieci. Tym samym zadbał doktorant o swego rodzaju uniwersalność proponowanego rozwiązania sieciowego: jedyną zmianą jest zmiana wartości wag, a nie struktury układu. Wobec tego doprowadzenie, na przykład do sytuacji, że proponowany układ realizuje konkretny S-blok, wymaga przeprowadzenia procesu uczenia z określonym zbiorem trenującym, a nie wymaga przebudowy struktury sieci.

Na zakończenie recenzji stwierdzam, że rozprawa mgr. Piotra Kotlarza zawiera oryginalny dorobek naukowy doktoranta, a wkład, jaki jej wyniki niosą do uprawianej przez Niego dyscypliny naukowej, jest bardzo wartościowy.

Należy na zakończenie tego punktu stwierdzić, że teza pracy o istnieniu alternatywego dla obecnie powszechnego podejścia do implementacji algorytmów kryptograficznych i wykorzystującego konstrukcje sztucznych sieci neuronowych, jednego z narzędzi inteligencji obliczeniowej (dawniej zwanej – sztuczną inteligencją), została wykazana.

Uwagi krytyczne i dyskusyjne

1. Mam kilka pytań do początkowego rozdziału:
   1. str. 9 , w.11 od dołu (o.d.) czy to równananie jest prawdziwe?
   2. str. 19 w.2 o.g. Pojawia sie E czy to jest F? Podobne pytanie jest do str. 24 i 25.
   3. str. 21: czy $D_k(z) = z$, dla każdego z ?

4. str. 26: W sumie nie widzę definicji S-bloku.
5. str. 27. Coś sie nie zgadza z tym złożeniem permutacji p_1, p_2; mnie wychodzi co innego. Coś z definicją cyklu też się nie zgadza we wskaźnikach na dole strony.

2. W definicji funkcji afinicznej na str. 30 nie wiadomo skąd pochodzą zmienne x_i w tym wzorze: czy takie jak α na górze strony? Autor przepisł ostatnią zależność z książki poz. [32], gdzie też zapomniano o oznaczeniu mnożenia modułowego przez $\odot$. W ten sposób pojawia się pytanie o zapis $a_i x_i$ i supozycja, że mamy do czynienia z mnożeniem bitów przez bajty.

3. Na str. 9 błędnie zapisano kolejność złożenia funkcji szyfrującej F i deszyfrującej D.

4. Na stronach 30 i 31 nazwisko Hamminga występuje w błednym zapisie, kilkakrotnie.

5. Na str. 31 : co oznacza rodzajnik *jej* w definicji nieliniowości?

6. Na str. 59 autor pisze o sieci CP, a potem używa skrótu sieć S-P. Należy oczekiwać, że jest to samo. Recenzent dla sprawdzenia wiedzy doktoranta prosi na publicznej obronie o przytoczenie defincji, charakteryzacji, tego typu sieci.

7. Na str. 67 na Rys. 6.17 próg ma wartość 7. Z moich obliczeń wynika, że powinien mieć wartość podwojoną.

   Poniżej na Rys. 6.18 zaznaczono przedział zmienności zmiennej x_1 jako $[1, 16]$. Tymczasem już wcześniej przyjęto przedział $[0, 15]$. Znów jest niekonsekwencja.

8. Opis w p. 6.3.3 redukcji 8 wejćć do czterech przy zachowaniu sposobu działania całego układu nie jest jasny. W szczególności niejasne jest: jak powstaje wyjście Y opisane ostatnią kolumną w Tabeli 6.13.

9. Układ (moduł) "dec2dec" wersja 2 opisany Rys. 6.32 wymaga dwóch wejść: x_1 i x_2. Należy oczekiwać, że jedno z nich jest stałe i równe 1. O tym autor nie pisze. Tymczasem na Rys. 6.33, który opisuje całą sieć z tym układem w środku, ma tylko jedno wejść do tego modułu. Sprawa wymaga wyjaśnienia.

10. Na str. 81 autor pisze: *Na jednym z 16 wyjść drugiej warstwy może pojawić się tylko jedna wartość różna od 0, w przypadku S-bloku algorytmu DES jest to wartość od 0-15.* Ale zero należy do zbioru wartości

0-15. Więc nie jest to 16 wartości. Z takim lapsusem łączy się zasadnicze pytanie: skoro wartość zero dla szyfru nie jest uprzwilejowana, natomiast dla sieci neuronowych jest, jak sobie doktorant daje radę z tą mała sprzecznością?

Proszę o ustosunkowanie się do tych uwag.

Uwagi końcowe

Przesłana do mnie do recenzji rozprawa doktorska mgr. Piotra KOTLARZA p.t. Sieci neuronowe we wspomaganiu rozwiązywania problemów kryptolgii promotorstwa doc. dr. hab. Zbigniewa Kotulskiego, spełnia wszystkie wymogi stawiane rozprawom doktorskim (Ustawa o stopniach naukowych i o tytule naukowym oraz o stopniach i tytule w zakresie sztuki z dnia 14 marca 2003 roku, Dziennik Ustaw Nr 65, poz. 595) w dziedzinie nauk technicznych w dyscyplinie informatyka. W związku z tym wnioskuję o dopuszczenie doktorant Pana mgra Piotra Kotlarza do dalszych etapów przewodu doktorskiego.