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.

2. Ocena rozprawy doktorskiej

2.1 Treść rozprawy

Praca składa się z 10 rozdziałów, bibliografii obejmującej 75 pozycji literaturowych, spisu rysunków oraz spisu tabel. W pierwszej części, obejmującej rozdziały 1-5, autor formułuje cel pracy oraz wprowadza czytelnika do problematyki kryptografii i sieci neuronowych. Druga część, obejmująca rozdziały 6-9, prezentuje własne oryginalne koncepcje zawiązane z zastosowaniem sieci neuronowych do tworzenia narzędzi kryptograficznych. Ostatni rozdział zawiera podsumowanie pracy.

Rozdział 1 pracy zawiera rys historyczny mający charakter wprowadzenia do zagadnień nowożytnej kryptografii i kryptologii. Doktorant przedstawia w nim również cel pracy, jej zakres i tezę pracy, a także omawia strukturę pracy doktorskiej.

Rozdział 2 pracy przedstawia elementy kryptografii, w tym koncepcje szyfrowania symetrycznego oraz szyfrowania asymetrycznego.

Rozdział 3 zawiera podstawy matematyczne dotyczące dwóch najważniejszych aspektów pracy: kryptografii oraz sieci neuronowych. Zdefiniowano pojęcie permutacji oraz pojęcie S-bloku jako funkcji boolowskiej. Określono kryteria projektowe, które musi spełniać funkcja boolowska, aby móc pełnić rolę S-bloku. Następnie wprowadzono w pracy pojęcie neuronu i przedstawiono jego model. Przestawiono proces uczenia się neuronu wykorzystujący regułe perceptronu oraz regułę Hebba, a następnie omówiono koncepcję sieci neuronowych oraz sieci logicznych realizujących funkcje boolowskie.

Rozdział 4 to krótki rozdział poświęcony omówieniu metod implementacji programowych i sprzętowych współczesnych szyfrów.

Rozdział 5 to również krótki rozdział będący przeglądem prac dotyczących wykorzystania sieci neuronowych w kryptografii.

Rozdział 6 jest pierwszym rozdziałem pracy przedstawiającym wyniki własne doktoranta. Na wstępie rozdziału doktorant zaproponował i przedstawił koncepcję realizacji permutacji na 2, 3 i 4-ch bitach z użyciem sieci boolowskiej. Dalsza część rozdziału poświęcona jest przedstawieniu koncepcji i realizacji S-bloku za pomocą sieci neuronowych. Pierwowzorem takiego bloku, który doktorant zamierzał realizować jest S-blok istniejący w algorytmie DES, będący tablicą o 4 wierszach i 15 kolumnach. Przedstawiona w tym rozdziale koncepcja realizacji S-bloku zakłada realizację, w pierwszym etapie, pojedynczego wiersza S-bloku, a następnie w drugim etapie, rozbudowa tej konstrukcji pojedynczego wiersza do pełnego S-bloku składającego się z 4 wierszy. Zaproponowana przez doktoranta koncepcja realizacji pojedynczego wiersza S-bloku wykorzystuje koncepcję sieci neuronowej przesyłającej żeton, tzw. sieci CP. Pełna realizacja S-bloku z użyciem sieci neuronowych wymagała od doktoranta rozwiązania szczegółowych problemów, takich jak konstrukcja neuronowej tablicy prawdy (oznaczana jako „4-kl") oraz modułu „p-w-d", konstrukcja neuronowego dekodera wartości dziesiętnych na binarne

(„dec2bin") oraz redukcja liczby wejść sieci neuronowej do 4-ch i związane z tym problemy konstrukcji dekoderów „bin2bin" czy „dec2dec". Niektóre z tych rozwiązań przedstwiono w kilku wariantach. W rozdziale tym przedstawiono również istotne z punktu widzenia pracy S-bloku zaimplementowanego z użyciem sieci neuronowej aspekty uczenia modułów sieci, bezpieczeństwa układu oraz jego wydajności.

W rozdziale 7 przedstawiono koncepcję kompletnego algorytmu szyfrującego zbudowanego z wykorzystaniem zaproponowanych w poprzednim rozdziale neuronowych implementacji permutacji oraz S-bloków. W charakterze takiego algorytmu wybrano trzyrundowy szyfr kaskadowy tzw. sieć podstawień i permutacji, składający się z 2 S-bloków oraz jednej permutacji, operujący na 24-ch wejściowych ciągach bitowych i wykorzystujący 12 bitowy klucz.. Przedstawiono również wyniki procesu uczenia S-bloku w tym szyfrze oraz pokazano parametry ilościowe neuronowej implementacji szyfru, tzn. liczbę neuronów oraz wag niezbędnych do realizacji permutacji i S-bloków.

W rozdziale 8 doktorant analizuje możliwości wykorzystania neuronowego szyfratora jako uniwersalnego układu szyfrujacego. Uniwersalność zaproponowanego neuronowego układu szyfrujacego polega na możliwości przeprogramowania wiedzy znajdującej się w posiadaniu sieci neuronowej i nabytej w procesie jej trenowania. Ta potencjalna możliwość sieci neuronowej umożliwia np. tworzenie S-bloków o innej zawartości aniżeli te stosowane w algorytmie DES. Doktorant analizuje możliwości przeprowadzenia procesu uczenia sieci dla dwóch przypadków: gdy uczenie odbywa się na serwerze, w którym znajduje się sieć neuronowa oraz gdy proces uczenia odbywa się po stronie klienta. Dla obu przypadków uczenia ukazuje on zbiór warunków jakie muszą być spełnione, aby uczenie miało miejsce i aby ten proces był bezpieczny.

Rozdział 9 poświęcony jest możliwościom praktycznego wykorzystania neuronowego szyfratora. Doktorant proponuje wykorzystanie zbudowanych neuronowych elementów układu szyfratora bądź ich modyfikację w celu wykorzystania ich (a) jako kluczy sesji, (b) kluczy dla dla pojedynczych cykli szyfrowania oraz (c) realizacji szyfrów tajnych.

W ostatnim rozdziale, rozdziale 10 przedstawiono podsumowanie rozprawy oraz wskazano dalsze kierunki rozwoju prowadzonych prac.

2.2 Najważniejsze wyniki uzyskane w rozprawie

Celem postawionym w rozprawie było zbadanie możliwości realizacji układów szyfrujących z użyciem sieci neuronowych. Ten cel jest bardzo interesujący, a przedstawione w rozprawie wyniki potwierdzają tezę o możliwości realizacji szyfratorów wykorzystujących w swoim działaniu sieci neuronowe. Realizacja tego celu wymagała rozwiązania szeregu problemów szczegółowych. W związku z tym do najważniejszych osiągnięć pracy związanych z realizacją postawionego celu można zaliczyć:

- opracowanie dwóch rozwiązań realizacji w postaci sieci neuronowej (neurony z wagami zmienoprzecinkowymi oraz neurony boolowskie) operacji permutacji
- opracowanie rozwiązania w postaci sieci neuronowej układu realizującego funkcję S-bloków
- realizacja za pomocą sieci neuronowych układu szyfrującego realizującego szyfrowanie kaskadowe

- opracowanie koncepcji protokołu kryptograficznego umożliwiającego stosowanie opracowanych rozwiązań w systemach sieciowych
- stworzenie oryginalnego oprogramowania umożliwiającego tworzenie i badanie rozwiązań kryptograficznych wykorzystujących sieci neuronowe.

2.3 Uwagi krytyczne

W trakcie zapoznawania się z rozprawą doktorską pojawiły się następujące uwagi odnoszące się do merytorycznych aspektów pracy, na które z przyjemnością usłyszałbym bardziej szczegółowe informacje :

- zbiór uczący stosowany w procesie uczenia sieci neuronowej implementującej permutację (str. 53) podany w tabeli 6.1 zawiera kilka elementów, natomiast proces uczenia przedstawiony na rys. 6.4 trwa kilkadziesiąt epoch. Jak wyglądały w związku z tym sekwencje uczące podawane na wejście sieci w trakcie jej uczenia ? Jak był definiowany błąd sieci przedstawiony na rys. 6.4 ? Jaki był wynik testowania sieci w świetle różnego od zera błędu sieci w trakcie jej uczenia ?
- jakie były wyniki uczenia i testowania sieci realizujących permutacje liczby bitów większej niż 2 i przedstawionych na str. 54-57 ?
- w trakcie opisu realizacji neuronowej S-bloku, a w szczególności podczas analizy przebiegu procesu uczenia układu „dec2dec" (rys. 6.26, str. 74) doktorant stwierdza, że „co prawda błąd nie osiągnął wartości 0, ale kontrola działania sieci zbiorem testującym dała zadawalające wyniki". Jakie wyniki w tym kontekście uważane są za zadowalające ?
- jaki jest końcowy efekt kumulacji błędów uczenia poszczególnych składowych podczas pracy opracowanego urządzenia szyfrujacego ?

Przestawione wyżej uwagi nie wpływają znacząco na moją pozytywną ocenę rozprawy.

2.4 Ocena redakcji rozprawy

Praca zredagowana jest przejrzyście, a wywód poprowadzony jest logicznie. Styl językowy pracy nie budzi zastrzeżeń. W trakcie czytania pracy zauważyłem pewną liczbę niedociągnięć redakcyjnych:

- na str. 1 jest 'implantacji' zamiast 'implementacji'
- na str. 30 jest 'Hemminga' zamiast 'Hamminga'
- na str. 33 i 36 jest 'neurony' zamiast 'neuronu'
- na str. 35 – niezręczne sformułowanie 'Po koncepcji perceptronu .. Heb zaproponował'
- na str. 48 jest 'kryptoalizę' zamiast 'kryptoanalizę'
- na wykresie z rys. 6.4, str. 53 oraz innych podobnych wykresach brakuje opisu jednostek w jakich jest skalowana oś x
- na str. 62 jest 'Ważny' zamiast 'Ważnym'
- na str. 100 jest 'wyniki' zamiast 'wyniku'
- na str. 103 jest 'bolok' zamiast 'blok'

3. Konkluzja

Postawione w rozprawie cele zostały przez doktoranta osiągnięte. Opracował on w sposób kompleksowy oryginalne podejście do realizacji systemów kryptograficznych wykorzystujące sieci neuronowe i pokazał jego praktyczną przydatność. Wyniki pracy były przedstawiane na kilku międzynarodowych konferencjach i publikowane w materiałach tych konferencji, w tym przez wydawnictwo Springer. Trzy artykuły został również opublikowany w czasopismach.

Podsumowując, uważam, że recenzowana rozprawa zawiera oryginalne i interesujące wyniki teoretyczne jak i praktyczne. Uzyskane wyniki stanowią znaczący wkład doktoranta do teorii i praktyki problematyki związanej z bezpieczeństwem kryptograficznym oraz sieciami neuronowymi.

Jestem przekonany, że wymagania stawiane rozprawom doktorskim przez obowiązującą Ustawę o Stopniach i Tytułach Naukowych zostały w pełni spełnione. Wnoszę więc o dopuszczenie mgr Piotra Kotlarza do publicznej obrony jego pracy.