

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 głośniejszych dziedzin informatyki. Szybki rozwój mocy obliczeniowych współczesnych komputerów jest ciągłym 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 szyfrowania np. bieżących rozmów telefonicznych w sieciach komórkowych, czy też do szyfrowania danych technicznych przesyłanych między współpracującymi urządzeniami (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 się 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 szyfrującego 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 związane 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. Przystawiono proces uczenia się neuronu wykorzystujący regułę 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-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

