Prof. dr hab. inż. Sebastian Deorowicz
Katedra Algorytmiki i Oprogramowania
Wydział Automatyki, Elektroniki i Informatyki
Politechnika Śląska
44-100 Gliwice, ul. Akademicka 16

Gliwice, 1.09.2022 r.

Recenzja rozprawy doktorskiej

Tytuł rozprawy:
Algorytmy memetyczne w kryptoanalizie różnicowej symetrycznych szyfrów blokowych

Autor:
mgr Kamil Dworak

Promotor:
Prof. Dr hab. Urszula Boryczka

Problematyka rozprawy

Ukrywanie informacji przed dostępem przez osoby niepowołane stosuje się od tysięcy lat. W tym czasie techniki szyfrowania przeszły dramatyczne zmiany od bardzo prostych metod o nikłej skuteczności do metod zapewniających bardzo duże bezpieczeństwo. Co więcej, obecnie techniki takie jak standardy szyfrowania DES, RSA i inne dostępne są praktycznie dla każdego. Z jednej strony daje to poczucie bezpieczeństwa i prywatności, ale z drugiej łatwo może prowadzić do zbytniej pewności siebie. Cały czas trwają bowiem prace mające na celu wyszukiwanie słabości istniejących metod szyfrowania czy też wprost metod ich łamania. Metody kryptoanalityczne mogą zapewnić znaczną przewagę czy to w gospodarce czy też w zastosowania wojskowych. Na przestrzeni wieków wielokrotnie okazywało się, że metody szyfrowania uchodzące za bezpieczne były łamane. Co więcej, informacja o ich złamaniu była często ukrywana przez bardzo długi czas, co pozwalało na długotrwałe odczytywanie informacji zaszyfrowanych przez przeciwników, którzy nie byli niczego świadomi.

Kryptoanaliza ma bardzo duże znaczenie także w związku z tym, że próby łamania stosowanych obecnie metod szyfrowania mogą prowadzić wczesnego wykrycia niebezpieczeństw związanych ze stosowaniem danej metody. Nieudane próby złamania szyfru stanowią także przesłankę za tym, że szyfr jest bezpieczny. Nie jest to żaden dowód na jego bezpieczeństwo, ale jednak zawsze lepiej mieć świadomość stosowania metody szyfrującej, której nie udało się złamać wielu osobom mimo prób, niż polegać na metodzie szyfrowania, o bezpieczeństwie której niewiele wiadomo.

Oceniana rozprawa podejmuje próbę opracowania metod kryptoanalizy popularnych algorytmów szyfrujących FEAL oraz DES. W tym celu wykorzystano kryptoanalizę różnicową oraz ewolucyjne algorytmy optymalizacyjne.

Analiza treści rozprawy oraz uzyskanych wyników

Treść rozprawy

Doktorant postawił sobie w pracy cel opracowania lepszych metod łamania szyfrów FEAL i DES. Wykorzystał przy tym wiedzę o istniejących słabościach tych metod szyfrowania, co pozwoliło na obranie potencjalnie skutecznego kierunku ataku.

Rozprawa napisana jest w języku polski i składa się z 8 rozdziałów oraz kilku dodatków. W pierwszym rozdziale Doktorant wprowadza czytelnika w problematykę, której dotyczy rozprawa, stawia tezę oraz formułuje cele szczegółowe.

Rozdział drugi stanowi wprowadzenie w tematykę kryptografii i bezpieczeństwa informacji. Znajdziemy tu definicje podstawowych pojęć czy też klasyfikację metod kryptograficznych. Następnie przedstawione są wybrane algorytmy symetryczne takie jak FEAL i DES, które będą analizowane w dalszej części pracy. Krótko omówione są także podstawowe metody kryptoanalizy, w tym kryptoanaliza różnicowa, kluczowa dla prac Doktoranta.

Kolejne dwa rozdziały opisują wybrane metody optymalizacji ewolucyjnej. W szczególności, w rozdziale trzecim przedstawiono algorytm genetyczny. Rozdział czwarty zawiera omówienie algorytmu memetycznego wraz z przeglądem wybranych technik przeszukiwania lokalnego.

Kolejne trzy rozdziały stanowią opisują autorski wkład w problematykę. W rozdziale piątym Doktorant przedstawia opracowane przez siebie metody ataku na algorytmy FEAL i DES. Obie metody korzystają ze znanych słabości tych algorytmów wykrytych dzięki kryptoanalizie różnicowej. Na tej bazie Autor zaproponował metody memetyczne pozwalające znacznie zawęzić przestrzeń poszukiwań klucza użytego do szyfrowania. W rozdziale szóstym Doktorat przedstawił wyniki badań eksperymentalnych zarówno własnych metod, NEA oraz MASA, jak i znanej z literatury metody DPSO. Rozdział siódmy zawiera porównanie uzyskanych wyników.

Ostatni rozdział stanowi podsumowanie. Doktorant przypomina tutaj postawioną tezę. Omawia uzyskane wyniki wskazując najważniejsze zrealizowane cele szczegółowe. Następnie konkluduje, że zarówno teza została udowodniona, jak i cele szczegółowe zostały osiągnięte.

Bibliografia rozprawy składa się ze 107 pozycji.

Najważniejsze wyniki przedstawione w rozprawie

Istotną rozprawy są dwie, zaproponowane przez Doktoranta, metody łamania metod szyfrowania FEAL oraz DES. Rozważane problemy mają duże znaczenie i z tego powodu prace Doktoranta mogą przyczynić się do opracowania lepszych metod szyfrowania poprzez lepsze zrozumie jakie techniki łamania szyfrów są skuteczne dla popularnych, stosowanych w praktyce metod szyfrowania.

Głównym osiągnięciem Doktoranta jest opracowanie algorytmu MASA, który wykorzystując kryptoanalizę różnicową, może być wykorzystany do wyraźnego przyspieszenia ataku na algorytm DES. Algorytm MASA łączy techniki kryptoanalizy różnicowej oraz algorytmu memetycznego, w którym do przeszukiwania lokalnego wykorzystano metodę symulowanego wyżarzania. Wyniki eksperymentalne pokazują, że algorytm MASA jest skuteczny dla uproszczonego do 6 rund szyfrowania DES a czas jego działania liczony jest w godzinach.

Uwagi merytoryczne

Praca zawiera dość dobre wprowadzenie w tematykę zarówno algorytmów ewolucyjnych wykorzystywanych do optymalizacji, jak i wybranych metod kryptoanalizy. Bibliografia zawiera reprezentatywne dla dziedziny publikacje. Struktura pracy jest poprawna. Autor przechodząc od definicji, poprzez omówienie stanu wiedzy przygotowuje czytelnika na przedstawienie własnych propozycji, które następnie poddawane są ocenie eksperymentalnej.

Mam jednak pewne uwagi krytyczne i prosiłbym o odniesienie się do nich w trakcie publicznej obrony.

1. Rysunek 5.4 pokazuje popularność technik metaheurystycznej kryptoanalizy na przestrzeni ostatnich lat. Nie jest to jasno powiedziane w tekście pracy, ale wnioskuję, że zwrócone wyniki z bazy Google Scholar dotyczą liczby publikacji na ten temat. Wydaje się zatem, że w ostatnich latach pojawiło się ok. 2000 takich prac. Tymczasem w trakcie ewaluacji opracowanych przez siebie metod Doktorant wykorzystał tylko 1 algorytm znany z literatury, który nie jest Jego autorstwa. Dlaczego się tak stało? Z pewnością porównanie z innymi metodami (o ile ich implementacje są dostępne) poprawiłoby część eksperymentalną pracy.
2. W pracy skupiono się (oprócz dość łatwego do kryptoanalizy algorytmu FEAL) tylko na uproszczonej wersji algorytmu DES. Ograniczenie na liczbę rund (6 zamiast 16) jest dość istotne. Biorąc pod uwagę dość dobre czasy działania algorytmu MASA zastanawiające jest dlaczego nie podjęto próby ataku na bardziej złożoną wersję algorytmu DES. W szczególności, interesująca by była próba odpowiedzi na pytanie czy uzyskane wyniki mają szanse być w jakikolwiek sposób uogólnione na kompletny (16-rundowy) algorytm DES. Nie oczekuję tutaj zaproponowania gotowego rozwiązania, ale chciałbym poznać opinię Doktoranta dotyczącą takiej możliwości oraz potencjalnych problemów.
3. Algorytmy memetyczne pozwalają na wykorzystanie różnych technik optymalizacji lokalnej. W rozprawie skupiono się jedynie na symulowanym wyżarzaniu. Chciałbym dowiedzieć się czy eksperymentowano z innymi technikami. Jeśli tak, to jakie były wyniki. Jeśli nie, to czym był podyktowany wybór metody symulowanego wyżarzania.

Uwagi redakcyjne

Ogólna kompozycja rozprawy jest poprawna. Sposób składu tekstu także jest poprawny. Wyjątkiem jest tutaj błędne stosowanie dywizu w miejscu, w którym powinna znajdować się pauza bądź półpauza. W większości tekst jest pisany poprawnym językiem, dość ścisłym. Niemniej w pracy pojawiają się także nieścisłości, czy błędne sformułowania. Poniżej przytoczę tylko niektóre z nich (jest ich niestety trochę więcej).

- [str. 8] „Przykład procesu szyfrowania z udziałem tekstu jawnego..." – przedstawiony rysunek nie pokazuje procesu szyfrowania a jedynie tekst wejściowy, klucz i tekst zaszyfrowany.
- [str. 8] „dowolnie odszyfrowany tekst" – nie jest jasne co Autor miał na myśli.
- [str. 8] „Współczesne algorytmy kryptograficzne można podzielić na trzy podstawowe grupy: [...] Jako czwartą grupę można zaliczyć nieużyteczną już dzisiaj kryptografię klasyczną". Autor sam (str. 6) pisze „Kryptografia jest dziedziną skupiającą się..." Tymczasem tutaj utożsamia kryptografię z grupą algorytmów a nie dziedziną.
- [str. 9] „Znaki występują nawet w tej samej liczbie, zmieniony jest jedynie ich układ i kolejność" – nie jest dla mnie jasne czym jest „zmiana układu znaków" a czym „zmiana kolejności znaków".
- [str. 10] „Do dwóch najpopularniejszych grup współczesnych algorytmów szyfrujących zalicza się algorytmy symetryczne oraz asymetryczne" – chyba chodziło o to, że to są te dwie grupy, a

nie, że algorytmy symetryczne i asymetryczne zalicza się do jakichś, nienazwanych nigdzie, grup.

- [str. 11] „Szyfry strumieniowe wykorzystywane są w sytuacji, gdy mamy do czynienia z nieokreślonym zbiorem danych, przesyłającym kolejne informacje w czasie rzeczywistym" – zbiór danych nie przesyła informacji.
- [str. 14] „Szyfr pracując na większych blokach danych staje się bezpieczniejszy, aczkolwiek traci na prędkości oraz wydajności podczas szyfrowania i deszyfrowania" – czym jest „prędkość" a czym „wydajność" i jaka jest między nimi różnica? Raczej chodzi też o „algorytm szyfrowania" a nie o „szyfr".

Takich przykładów jest sporo w całym tekście pracy, co wskazuje na pewną niestaranność Autora.

Podsumowanie

Przedstawiona do oceny rozprawa zawiera interesujące wyniki. Tematyka jest bez wątpienia ciekawa i ważna a podjęte próby stworzenia nowego podejścia do kryptoanalizy są godne pochwały. Uzyskane wyniki są obiecujące i choć same w sobie nie stanowią przełomu praktycznego (np. poddano tylko analizie mocno okrojoną wersję algorytmu DES oraz algorytm FEAL), to mogą one stanowić punkt wyjścia do dalszych, bardziej ambitnych prac, o czym wspomina także sam Doktorant w podsumowaniu.

Rozprawa zawiera pewne niedociągnięcia redakcyjne, co wskazałem w niniejszej recenzji. Tym niemniej moja ogólna ocena przedłożonej rozprawy jest pozytywna.

Baza Google Scholar odnotowuje 55 cytowań prac Doktoranta, z których spora część to cytowania innych badaczy. Świadczy to pozytywnie od odbiorze prac Autora, których podsumowaniem jest opiniowana rozprawa.

Konkluzja

Podsumowując opinie zawarte w mojej recenzji, mogę stwierdzić, że zgodnie z „Ustawą o Stopniach naukowych..." recenzowana rozprawa mgra Kamila Dworaka nt. „Algorytmy memetyczne w kryptoanalizie różnicowej symetrycznych szyfrów blokowych" stanowi oryginalne rozwiązanie problemu naukowego oraz wykazuje ogólną wiedzę teoretyczną kandydata w dyscyplinie informatyka techniczna i telekomunikacja oraz umiejętność prowadzenia pracy naukowej. Zawarte w recenzji uwagi krytyczne mają charakter dyskusyjny i nie wpływają na pozytywną ocenę rozprawy. Wnoszę zatem o dopuszczenie wspomnianej rozprawy do publicznej obrony.

Sebastian Deorowicz