Prof. dr hab. inż. Franciszek Seredyński
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
Wydział Matematyczno – Przyrodniczy
Szkoła Nauk Ścisłych
ul. Wóycickiego 1/3, 01-938 Warszawa

Warszawa, 20.10.2022

RECENZJA

rozprawy doktorskiej mgr Kamila Dworaka nt.
„Algorytmy memetyczne w kryptoanalizie różnicowej symetrycznych szyfrów blokowych"
w związku z ubieganiem się o uzyskanie stopnia doktora nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja

1. Problematyka naukowa oraz przedmiot rozprawy

Kryptograficzne metody zapewnienia bezpieczeństwa przekazywanej informacji są dzisiaj jednym z kluczowych elementów współczesnych technologii informatyczno-komunikacyjnych takich jak Internet, sieci telefonii komórkowej czy nowotworzone technologie oparte na koncepcjach Internetu Rzeczy. Istnieje swoisty wyścig między tworzonymi i aktualnie stosowanymi metodami kryptograficznymi oferującymi określony poziom bezpieczeństwa przekazywanej bądź chronionej informacji, a narzędziami i metodami zorientowanymi na zachwianie tego bezpieczeństwa. Dlatego zagadnienia kryptoanalizy, którymi zajmuje się Doktorant w swojej rozprawie, mającymi na celu odnalezienie słabości stosowanych szyfrów w celu ich złamania i odczytania zaszyfrowanej informacji są aktualnym problemem naukowym współczesnej informatyki uzasadniającym celowość podjęcia tego tematu w ramach pracy doktorskiej.

Problem poszukiwania słabości danego szyfru może być sprowadzony do poszukiwania optimum określonej funkcji w pewnej przestrzeni rozwiązań. Ze względu na istnienie bardzo dużych przestrzeni rozwiązań celowe jest zastosowane przez Doktoranta podejście oparte na poszukiwaniu rozwiązań problemu z użyciem metod metaheurystycznych, które umożliwiają odnalezienie dobrych przybliżonych rozwiązań w rozsądnym czasie.

W swojej rozprawie Doktorant skupił się na wykorzystaniu dla celów kryptoanalizy różnicowej symetrycznych szyfrów blokowych, jednej z metaheurystyk określanych jako algorytmy memetyczne. Postawionym celem rozprawy zawartym w tezie jest zbadanie czy i w jakim stopniu algorytmy memetyczne stosowane w kryptoanalizie różnicowej poprawiają efektywność stosowanych ataków kryptograficznych. Przedstawione w rozprawie wyniki w pełni potwierdzają tezę rozprawy.

2. Analiza treści rozprawy oraz uzyskanych wyników

Rozprawa składa się z 8 rozdziałów, bibliografii obejmującej 107 pozycji literaturowych, dwóch dodatków, spisu algorytmów, spisu rysunków oraz spisu tabel. Całość pracy obejmuje 153 strony i ma charakter teoretyczno-eksperymentalny. Najważniejsze rozdziały rozprawy to rozdziały 5, 6 i 7, które zawierają oryginalne wyniki Doktoranta.

Rozdział 1 stanowi wprowadzenie do problematyki rozprawy. Doktorant formułuje w nim tezę rozprawy, jej cel oraz przedstawia krótko treść poszczególnych rozdziałów.

W Rozdziale 2 Doktorant przedstawił podstawowe zagadnienia związane z kryptologią i bezpieczeństwem informacji. W szczególności przedstawił klasyfikację algorytmów kryptograficznych, zasady projektowania szyfrów blokowych oraz przedstawił szczegółowo dwa algorytmy kryptografii symetrycznej, które będą w rozprawie badane, a mianowicie algorytm FEAL oraz algorytm DES. Rozdział kończy się przeglądem podstawowych metod ataków kryptoanalitycznych, w tym kryptoanalizy różnicowej oraz kryptoanalizy liniowej.

W kolejnym rozdziale, Rozdziale 3 zostały przedstawione podstawy algorytmów ewolucyjnych. Doktorant omówił koncepcję algorytmu ewolucyjnego oraz szczegółowo przedstawił stosowane w algorytmie operatory.

Rozdział 4 poświęcony jest algorytmom memetycznym, które są głównym narzędziem stosowanym przez Doktoranta do poszukiwania rozwiązań problemu kryptoanalizy różnicowej. Algorytm memetyczny to algorytm hybrydowy, który łączy w sobie główne komponenty algorytmu ewolucyjnego oraz określoną metodę optymalizacji lokalnej. W ramach możliwych kandydatów puli metod optymalizacji lokalnej Doktorant przedstawia takie algorytmy jak algorytm wspinaczki, symulowane wyżarzanie oraz metodę tabu search.

Rozdział 5 jest pierwszym rozdziałem rozprawy, w którym przedstawiono wyniki własne związane z zastosowaniem algorytmów memetycznych do kryptoanalizy różnicowej. Doktorant przedstawia koncepcję ataku na szyfr FEAL, przedstawia proponowaną koncepcję kodowania osobnika algorytmu memetycznego, w postaci 32-bitowego łańcucha kodującego podklucze algorytmu szyfrującego oraz przedstawia proponowaną funkcję przystosowania, która ocenia rozwiązania. Jako algorytm lokalnego przeszukiwania Doktorant proponuje wykorzystać algorytm symulowanego wyżarzania. Następnie Doktorant modyfikuje zaproponowane podejście w celu wykonania ataku na bardziej zaawansowany algorytm kryptograficzny jakim jest DES. Zaproponowany algorytm memetyczny łączący algorytm ewolucyjny i symulowane wyżarzanie Doktorant określa jako MASA (ang. Memetic Algorithm Simulated Annealing). W końcowej części rozdziału Doktorant przedstawia inne znane z literatury algorytmy ewolucyjne, które były stosowane do problemu kryptoanalizy różnicowej, w celu ewentualnego porównania wyników. Wśród tych algorytmów jest wcześniejszy algorytm określany jako NEA, którego Doktorant jest współautorem, który był stosowany do kryptoanalizy szyfru FEAL. Dla potrzeb prowadzonych badań w ramach rozprawy doktorskiej algorytm NEA był rozbudowany o dodatkowy element, tzw. operator heurystycznej negacji. Doktorant przedstawia również inny algorytm znany z literatury jako DPSO, który wykorzystywał koncepcję tzw. optymalizacji stadnej i był wykorzystywany do ataku na algorytm DES. Jak rozumiem, algorytm ten był zaimplementowany przez Doktoranta w celu umożliwienia porównania wyników z wynikami uzyskiwanymi z jego własnym algorytmem.

Rozdział 6 zawiera wyniki badań eksperymentalnych wykonanych z użyciem zaproponowanego algorytmu memetycznego MASA, który został użyty w odpowiednich wersjach do wykonania ataku na szyfrogramy uzyskane z użyciem algorytmów kryptograficznych FEAL oraz DES. Uzyskane wyniki zostały porównane z wynikami uzyskanymi z użyciem innych algorytmów. W przypadku ataku na szyfrogamy FEAL był to inny autorski algorytm NEA, a w przypadku ataku na szyfrogramy DES wyniki porównano z wynikami algorytmu bazującego na opisanego w literaturze algorytmu DPSO. Szyfrogramy uzyskane przez FEAL oraz DES uzyskano z użyciem 5 kluczy szyfrujących.

Wyniki przeprowadzonych eksperymentów pokazały, że wyniki ataków na szyfrogramy FEAL oraz DES były porównywalne i w związku z tym w pracy pokazano tylko wyniki dla DES. Wyniki eksperymentów dla DES pokazują, że zaproponowany algorytm memetyczny MASA jest zdecydowanie bardziej skuteczny przy wykonywaniu ataków na DES niż wcześniejsza autorska wersja algorytmu NEA. Już pierwsze wyniki przedstawione w Tab. 6.5 pokazują, ze o ile algorytm MASA skutecznie wykonuje ataki na prawie wszystkie podklucze w 50 eksperymentach (za wyjątkiem jednego z nich), to algorytm NEA nie radzi sobie w 12 eksperymentach. Doktorant pokazuje szczegółowe wyniki eksperymentów (ataków) z użyciem MASA oraz NEA dla różnych klu-

czy/podkluczy, pokazując efektywność poprawnie odgadywanych bitów, która dla algorytmu MASA jest w zakresie (90% - 93%) oraz dla algorytmu NEA zakresie (53% - 90%). Wyniki te wskazują, że efektywność zaproponowanego algorytmu MASA jest znacznie wyższa niż algorytmu NEA. Wyniki przeprowadzonych eksperymentów z algorytmem DPSO nie są jednoznaczne, ale pokazują, że jego efektywność jest zdecydowanie gorsza niż efektywność autorskiego algorytmu.

W Rozdziale 7 Doktorant przedstawił wyniki analizy skuteczności opracowanych algorytmów pod kątem liczby sprawdzonych rozwiązań, czasu odszyfrowania kryptogramu oraz zużywanymi zasobami komputerowymi. Doktorant pokazuje, że dzięki zwiększonej częstotliwości poprawnie odgadniętych bitów proces kryptoanalizy w wykonaniu algorytmu MASA jest bardziej efektywny niż ma to miejsce w przypadku innych rozpatrywanych algorytmów i wymaga znacznie mniejszej liczby sprawdzania podkluczy. MASA wymaga więcej pamięci niż NEA, ale te wielkości są znacznie mniejsze niż w przypadku użycia np. kryptoanalizy różnicowej. Również MASA posiada znaczną przewagę nad innymi algorytmami klasycznymi, chociaż ustępuje w tym względzie algorytmowi NEA.

Ostatni z rozdziałów, Rozdział 8 jest podsumowaniem wyników osiągniętych w rozprawie oraz przedstawia propozycję dalszej kontynuacji badań.

3. Najistotniejsze osiągnięcia przedstawione w rozprawie

Rozprawa doktorska mgr Kamila Dworaka zawiera nowe, oryginalne wyniki dotyczące zastosowania algorytmów metaheurystycznych w kryptoanalizie różnicowej symetrycznych szyfrów blokowych. Do najistotniejszych osiągnięć rozprawy zaliczyć należy:

- Zaproponowanie dwóch algorytmów, algorytmu memetycznego MASA oraz algorytmu ewolucyjnego NEA umożliwiające ataki kryptoanalityczne na algorytmy kryprograficzne FEAL oraz DES,

- Przeprowadzenie obszernych eksperymentalnych badań pokazujących wysoką skuteczność tych algorytmów przy wykonywaniu ataków, w tym wykazanie szczególnych możliwości wykonywania efektywnych ataków przez algorytm MASA,

- Zaprojektowanie i implementacja platformy informatycznej umożliwiającej automatyczną kryptoanalizę różnicową,

- Obszerny przegląd literaturowy dotyczący istniejących metod i technik używanych do ataków kryptoanalitycznych.

4. Uwagi merytoryczne

W trakcie czytania rozprawy doktorskiej mgr Kamila Dworaka nasuwają się pewne uwagi, a mianowicie:

- W trakcie objaśniania koncepcji ataku memetycznego skierowanego na szyfr FEAL (patrz, podrozdział 5.1), Doktorant mówi o różnicy dowolnej pary bloków danych wejściowych i używa do tego celu notacji typu 0x800000 czy 0x02000000, ale nie wyjaśnia jednak tej notacji, co utrudnia czytelnikowi zapoznawanie się z pracą,

- Klasyczny algorytm memetyczny składa się z algorytmu metaheurystycznego, który operuje na całej przestrzeni rozwiązań oraz algorytmu lokalnego przeszukiwania, który nie jest metaheurystyką i którego zadaniem jest poprawa aktualnie najlepszego aktualnie osobnika w bieżącej populacji algorytmu heurystycznego w lokalnej przestrzeni tego osobnika. Doktorant wykorzystuje w charakterze algorytmu metaheurystycznego algorytm genetyczny (AG), natomiast w charakterze algorytmu lokalnego przeszukiwania proponuje inny algorytm metaheurystyczny, mianowicie algorytm symulowanego wyżarzania (SW), który operuje również na całej przestrzeni rozwiązań i algorytm ten stosuje do każdego osobnika populacji AG (patrz, Algorytm 7, str. 59). Jeżeli AG posiada populację składającą się z np. z 10 osobników (jak to ma miejsce w przypadku ataku na DES) oraz np. wykonuje się w przeciągu 100 iteracji, to jak rozumiem, algorytm SW jest uruchomiany 10 x 100 = 1000 razy, co prawdopodobnie prowadzi do bardzo kosztownych czasowo obliczeń,

- Nie jest jasne dlaczego Doktorant wybrał taka formę połączenia obu metaheurystyk, gdzie SW jest uruchomiany wielokrotnie; Za każdym uruchomieniem SA, niezależnie od osobnika AG, który jest dla algorytmu SA początkowym rozwiązaniem, algorytm SA powinien odnajdywać rozwiązanie bliskie do globalnego rozwiązania. Na wykresie (np. pokazanym na Rysunku 6.3) pokazującym przystosowanie w zależności od iteracji (generacji) AG oczekiwalibyśmy dla każdej generacji podobnego wyniku (ze względu na globalne działanie SW). Tak jednak nie jest, wyniki ulegają poprawie ze wzrostem liczby generacji. W jaki sposób można to wyjaśnić, jeżeli ogólnie wiadomo, że wynik działania SW nie zależy od początkowego rozwiązania podawanego przez AG czy inny algorytm ?

- Ponieważ algorytm MASA składa się z dwóch kolejno uruchomianych metaheurystyk to powstaje pytanie: jaki wpływ na rozwiązania ma każda z metaheurystyk uruchomianych oddzielnie. W związku z tzw. lunch theorem mogłoby się okazać, że do rozpatrywanego problemu bardziej nadaje się tylko jedna z tych metaheurystyk, lub być może, że obie mają podobną wydajność,

- Algorytm SW, jak się wydaje, jest stosowany w uproszczonej formie (patrz, Algorytm 7, str. 59), w tym sensie, że liczba losowych iteracji L przy danej temperaturze wynosi 1, co może wpływać na efektywność generowanych przez SA rozwiązań. Również wartość współczynnika wygaszania wynosząca 0.9 (wg. Tabeli 6.2, str. 69) jest być może zbyt mała i może wpływać na efektywność generowanych rozwiązań. W celu otrzymania dobrych wyników zwykle ta wartość jest nie mniejsza niż 0.95, co niestety znacznie wydłuża czas działania algorytmu.

Powyżej przedstawione uwagi mają charakter dyskusyjny nie mają istotnego wpływu na jakość i wagę przedstawionych rozwiązań i w żadnym stopniu nie obniżają wartości pracy. Doceniam wkład pracy Doktoranta przy realizacji pracy i uzyskane wyniki, jak też liczę na interesującą dyskusję w trakcie obrony pracy, podczas której z pewnością zostaną wyjaśnione moje uwagi. Reasumując można stwierdzić, że główne wyniki rozprawy potwierdzają osiągnięcie z powodzeniem założonego w rozprawie celu.

5. Uwagi redakcyjne i edytorskie

Uwagi redakcyjno-edytorskie są następujące:

- Str. 1: Doktorant podaje 3 rodzaje wymagań dotyczących spełnienia wymagań bezpieczeństwa systemów informatycznych – nie jest to lista kompletna,

- Str. 6: „Odbiorca, posługując się prostym przedmiotem..." – nie bardzo wiadomo o jaki „prosty przedmiot" chodzi,
- Str. 25: „Metody heurystyczne wykorzystywane są do głównie do optymalizacji problemu" – problem się rozwiązuje, a nie optymalizuje,
- Str. 26: programowanie genetyczne pozwala na automatyczne tworzenie programów komputerowych, ale programowanie ewolucyjne do tego nie służy,
- Str. 28: „Warunkiem koniecznym …staje się kodowanie …do takiej formy, aby była ona najbardziej przychylna" – zabawne
- W Algorytmie 7 (str. 59) są prawdopodobnie źle skierowane nierówności w wierszach 8, 10,14, 26,
- Str. 68: „wszystkie doświadczenia zostały wykonane" → „wszystkie eksperymenty zostały wykonane",
- Str. 83: brakuje w tekście 2 rysunków: Rys. 6.19 oraz Rys. 6.20,
- Str. 89: „można zauważyć straszne wahania" – zabawne, proszę nie straszyć,
- Str. 108: „wydanie spacjalne" –> „wydanie specjalne".

6. Podsumowanie

Podsumowując, stwierdzam, że przedstawiona do oceny rozprawa doktorska mgr Kamila Dworaka pt.: *„Algorytmy memetyczne w kryptoanalizie różnicowej symetrycznych szyfrów blokowych"* spełnia wymagania stawiane rozprawom doktorskim przez obowiązującą ustawę z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce i pozwala na ubieganie się o uzyskanie stopnia doktora nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja. Uzyskane w rozprawie wyniki były prezentowane na trzech międzynarodowych konferencjach oraz publikowane w materiałach tych konferencji w serii LNCS, wydawnictwa Springer. Jeden z artykułów opublikowano w wysoko punktowanym czasopiśmie *Entropy*. W konsekwencji stwierdzam, że rozprawa może stać się przedmiotem publicznej obrony i wnoszę o dopuszczenie mgr Kamila Dworaka do dalszych etapów przewodu doktorskiego. W związku z interesującymi wynikami uzyskanymi w rozprawie potwierdzonymi publikacjami, w szczególności w czasopiśmie z *Impact Factor* wynoszącym 2.642 (w 2021 r) wnoszę o wyróżnienie rozprawy.