Warszawa, 15.09.2022

Recenzja rozprawy doktorskiej „SAT-kryptoanaliza wybranych algorytmów kryptografii symetrycznej” autorstwa Sylwii Stachowiak

Tematyka rozprawy

Tematyka rozprawy dotyczy kryptoanalizy logicznej (zwanej również SAT-kryptoanalizą) wybranych szyfrów kryptografii symetrycznej. Ogólnie ujmując, metoda ta polega na translacji problemu bezpieczeństwa algorytmu kryptograficznego do problemu spełnialności (ang. SATisfiability) formuły boolowskiej. Autorka skoncentrowała swoją analizę na dwóch współczesnych szyfrach (AES i Salsa20) oraz standardzie DES. W ramach pracy przeprowadzono serię badań eksperymentalnych metodą SAT-kryptoanalizy z wybranym tekstem jawnym. Otrzymane wyniki pozwoliły wyznaczyć granice możliwości przeprowadzenia ataku na wyżej wymienione szyfry z wykorzystaniem kryptoanalizy logicznej.

Charakterystyka rozprawy

Poniżej przedstawiam ogólną charakterystykę rozprawy (cel, teza oraz struktura). Autorka określiła cztery cele szczegółowe:

1. Opracowanie i wdrożenie dla wybranych, charakterystycznych szyfrów symetrycznych nowych metod ich bezpośredniego kodowania do formuł boolowskich.

2. Przeprowadzenie serii badań eksperymentalnych łamania brutalnego szyfrów, ich

fragmentów i/lub modyfikacji metodą SAT-kryptoanalizy z tekstem jawnym i szyfrogramem.

3. Przeprowadzenie serii badań eksperymentalnych dla różnych wariantów S-boxów stosowanych w szyfrach symetrycznych i ich różnych metod kodowania.

4. Wyznaczenie dla badanych algorytmów szyfrujących granicy możliwości przeprowadzenia na szyfr ataku brutalnego metodą SAT ze względu na różne parametry szyfru.

Postawione cele spaja teza, którą Doktorantka sformułowała następująco:

„*Zastosowanie bezpośredniego kodowania boolowskiego oraz SAT-solverów jest efektywną metodą do badania własności szyfrów symetrycznych i ich modyfikacji, w tym do wyznaczania granicy możliwości przeprowadzenia na szyfr ataku brutalnego metodą SAT-kryptoanalizy z uwzględnieniem różnych parametrów i/lub modyfikacji szyfru.”*

Sformułowana teza jest spójna z postawionymi celami badawczymi, których realizacja powinna zweryfikować tezę. Moją wątpliwość budzi sformułowanie (przewijające się przez całą rozprawę) „atak brutalny metodą SAT”. W polskiej literaturze raczej używa się terminu „atak wyczerpujący” lub „siłowy”. Oznacza on przeszukanie całej przestrzeni kluczy, bez żadnego wglądu w szczegóły działania szyfru. Używając dodatkowych narzędzi (np. SAT-solvera) atak przestaje być atakiem na siłę, atakujący wykorzystuje wiedzę o specyfice algorytmu i próbuje skrócić czas ataku. Stąd sformułowanie „atak brutalny metodą SAT” jest, moim zdaniem, mylące.

Struktura rozprawy

Rozprawa podzielona jest na 6 rozdziałów.

Rozdział 1 wprowadza czytelnika w tematykę badań, określa cele, tezę oraz podsumowuje główne wyniki badań eksperymentalnych. Rozdział 2 stanowi wprowadzenie do kryptologii na potrzeby rozprawy oraz opisuje analizowane szyfry. Autorka również przybliża podstawowe techniki kryptoanalityczne w tym przede wszystkim kryptoanalizę logiczną oraz szczegóły działania SAT solverów.

Kolejny rozdział przedstawia kryptoanalizę SAT szyfru DES. Większość z prezentowanych tutaj treści to rozwiązania już wcześniej publikowane. Autorka szczegółowo wprowadza w problematykę kodowania bezpośredniego szyfrów do formuł boolowskich. Dodatkowo przedstawione są autorskie kodowania różnych wariantów Sboxów standardu DES i wyniki eksperymentalne (czas obliczeń).

W Rozdziale 4 został dokładnie umówiony szyfr Salsa20. Dalej Autorka proponuje kodowanie boolowskie szyfru stosując metodologię przedstawioną w poprzednim rozdziale. Rozdział kończy się omówieniem wyników SAT kryptoanalizy dla Salsa20 uzyskanych przez wybrane SAT-solvery.

W następnym rozdziale przybliżony jest szyfr AES wraz z matematycznym opisem poszczególnych kroków algorytmu. Podobnie jak dla wcześniej analizowanych algorytmów znajdziemy tutaj kodowanie kroków algorytmu oraz wiele eksperymentów pokazujących granice możliwości SAT solverów dla kryptograficznego standardu AES.
Rozprawa kończy się Podsumowaniem, gdzie omówione są wyniki i realizacja celów badawczych.

Uwagi ogólne

Tematyka pracy jest interesująca, należy podkreślić dbałość w wykonaniu i prezentacji eksperymentów. Pozytywny jest również fakt, że cześć wyników udało się opublikować, z czego najciekawsza wydaje się praca: Stachowiak S., Kurkowski M., and Soboń A., SAT-Based Cryptanalysis of Salsa20 Cipher, Progress in Image Processing, Pattern Recognition and Communication Systems, pp. 252-266, Springer International Publishing, 2021.

Kryptoanaliza z użyciem SAT solverów wykorzystywana jest już około dwóch dekad. Z dotychczasowych badań wynika, że skuteczność tej metody jest mocno ograniczona i zwykle udaje się złamać tylko pojedyncze rundy algorytmu. Analiza i eksperymenty z rozprawy potwierdzają wyniki wcześniejszych badań przeprowadzonych dla innych algorytmów. Z tego powodu bardziej interesujące byłoby osadzenie pracy w kontekście SAT solverów i algorytmów tam używanych.

Społeczność skupiona wokół konkursów na najlepsze SAT-solvery dostrzega trudność formuł CNF budowanych na bazie problemów krytpograficznych. Świadczy o tym osobny „track" na jednym z konkursów https://satcompetition.github.io/2021/track_crypto.html

Uwagi szczegółowe

Wyniki eksperymentalne (czasy obliczeń) podawane są w pracy w sekundach (lub informacja o niezakończeniu obliczeń w zakładanym limicie czasowym np. 24 godziny). Brakuje w pracy przeliczenia czasu na złożoność (chociażby w przybliżeniu). Wtedy łatwiej ocenić czy dany atak faktycznie jest lepszy od przeszukiwania na siłę. Informacja, że SAT-solver obliczył brakujące 40 bitów w 6 godzin nie mówi wiele.

W pracy często po formule boolowskiej wygenerowana jest ta sama formuła tyle, że w formacie DIMACS. Jednorazowe pokazanie jak wygląda zapis formuł CNF dla SAT-solverów (format DIMACS) w zupełności by wystarczyło.

Rozdział poświecony standardowi DES jest w mojej ocenie zdecydowanie zbyt obszerny. Szyfr ten ma blisko 60 lat, pojedynczy DES nie jest (nie powinien) być stosowany, dużo ciekawsza byłaby analiza innego, bardziej współczesnego algorytmu.

Pewnym problemem w pracy jest terminologia, a w zasadzie tłumaczenie terminów anglojęzycznych na język polski. Przykładowo „metoda brutalna" nie brzmi dobrze, w polskiej literaturze spotykamy raczej „przeszukiwanie wyczerpujące" czy „na siłę". Na usprawiedliwienie Autorki należy zaznaczyć, że problem ten jest powszechny i wszędzie tam gdzie dziedzina wiedzy jest dynamiczna, rodzima terminologia nie ma szansy okrzepnąć (a czasem w ogóle nie pojawiają się pozycje w języku polskim).

Konkluzja

Uważam, że złożona rozprawa mgr Sylwii Stachowiak spełnia wymagania ustawowe i zwyczajowe stawiane pracom doktorskim i może stanowić podstawę nadania stopnia doktora w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja.

Paweł Kowalski