In Confidence

Professor Josef Pieprzyk, PhD, DSc
Senior Principal Research Scientist
Data61, CSIRO
Distributed Systems Security
Cnr Vimiera and Pembroke Roads
Marsfiled, NSW 2122
PO Box 76, Epping NSW 1710, Australia
email: *josef.pieprzyk@csiro.au*

Recenzja Rozprawy Doktorskiej

20 września, 2022

SAT-kryptoanaliza Wybranych Algorytmów Kryptografii Symetrycznej
Mgr Sylwia Stachowiak, SGGW, Warszawa

Wprowadzenie

Tematyką rozprawy jest kryptoanaliza szyfrów symetrycznych. Kryptoanaliza jest jednym z najbardziej aktywnych i rozwijających się działów współczesnej kryptologii. Do głównych narzędzi kryptoanalizy należy zaliczyć analizę różnicową, liniową oraz algebraiczną. Przedstawioną w pracy analizę za pomocą narzędzi SAT można potraktować jako fragment kryptoanalizy algebraicznej.

Praca składa się z następujących rozdziałów. Rozdział 1 przedstawia cele i uzyskane wyniki badawcze. Rozdział 2 wprowadza czytelnika do kryptologii oraz problemu spełnialności (ang. satisfiability problem). Nazwy problem spełnialności oraz problem SAT są w tej recenzji używane zamiennie. Rozdziały 3, 4 i 5 zawierają oryginalne przyczynki autorki. I tak rozdział 3 opisuje wyniki kryptoanalizy szyfru DES (ang Data Encryption Standard) z użyciem programu komputerowego, który jest zaprojektowany do rozwiązywania instancji problemu SAT. W pracy program ten jest nazywany SAT solverem. Rozdział 4 przedstawia kryptoanalizę szyfru Salsa20. Użytym narzędziem jest SAT solver. Rozdział 5 kontynuuje analizę, ale tym razem jest to szyfr AES (ang. Advanced Encryption Algorithm). Rozdział 6 zamyka rozprawę podsumowaniem uzyskanych wyników badawczych.

Oryginalny Wkład

Poniższa lista wskazuje na oryginalne przyczynki badawcze zawarte w rozprawie. Są to:

- rozszerzenie kryptoanalizy szyfru DES w oparciu o nowe SAT solvery. Rezultaty tych badań zostały opublikowane w materiałach konferencyjnych (Stachowiak S., Kurkowski M., and Soboń A., *SAT vs. Substitution Boxes of DES like Ciphers*, 2021 IEEE 30th International Conference on Enabling Technologies, WETICE, 2021, pp. 113-118);
- kryptoanaliza szyfru Salsa20 zawierającego co najwyżej 4 rundy wraz z określeniem praktycznej granicy złożoności obliczeniowej ataków z użyciem SAT solverami. Ta część pracy jest opublikowana w materiałach konferencyjnych (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, 2021);

- kryptoanaliza jednorundowego szyfru AES. Wyniki tych badań są przygotowywane do publikacji (prace [127] oraz [128] podane w bibliografii).

Szczegółowe Uwagi i Komentarze

Jak zauważyliśmy na samym wstępie, kryptoanaliza wykorzystująca algorytmy zaprojektowane do rozwiązywania instancji (lub przypadek) problemu spełnialności (SAT) można traktować jako część szeroko rozumianej analizy algebraicznej. Zauważmy, że klasa problemów **NP** zawiera wszystkie problemy (decyzyjne), których rozwiązania mogą być zweryfikowane w czasie wielomianowym. Z tego wynika, że wszystkie efektywne algorytmy kryptoanalizy muszą należeć do klasy **NP**. W szczególności, kryptoanaliza różnicowa i liniowa należą do klasy **NP**. Tutaj napotykamy na oczywiste trudności techniczne. Po pierwsze, konkretny algorytm kryptoanalizy musi być zredukowany do odpowiedniego problem decyzyjnego. Po drugie, otrzymana redukcja wielomianowa powinna być na tyle efektywna, aby pozwalała na praktyczne łamanie szyfru. Kryptoanaliza przedstawiona w rozprawie nie odnosi się do żadnej szczególnej analizy (różnicowej lub liniowej). Prezentowane podejście polega na zakodowaniu pojedynczych rund szyfrów w instancje problemu SAT. Inaczej mówiąc, poszczególne części składowe szyfrów są przedstawione w koniunkcyjnej postaci normalnej (CNF). Niestety, SAT solvery nie akceptują formuł CNF. Istnieje więc potrzeba ich przetłumaczenia na powszechnie używany przez solvery format DIMACS.

Rozdział 3 rozprawy analizuje szyfr DES. Chociaż DES przestał być standardem, to jednak ciągle jest on nie tylko przedmiotem zainteresowania ale również znakomitym szyfrem do testowania różnych ataków. Jak wiadomo, DES ma strukturę Feistela opartą o następujące operacje: permutacji, kompresji, rotacji i rozszerzenia. Osiem skrzynek (S-boxów) algorytmu DES można zakodować używając kodowanie czterech permutacji zdefiniowanych dla nich. W pracy pokazano szczegóły kodowania. Opisana część teoretyczna poprzedza bogaty zestaw eksperymentów z różnymi wersjami szyfru DES z użyciem jedno oraz wielowątkowych SAT solverów. Do najbardziej interesujących wyników należy zaliczyć kryptoanalizę szyfru DES z pełną liczba (16) rund i ze znanymi 38 bitami klucza. Prowadzi to do (prawie) praktycznego ataku probabilistycznego o złożoności obliczeniowej $2^{38}\alpha$, gdzie α jest to czas potrzebny do rozwiązania pojedynczego przypadku przez SAT solver. Nie jest zaskoczeniem fakt, że kryptoanaliza szyfru z SAT solverami jest nieskuteczna, gdy wszystkie bity szyfru są nieznane.

Rozdział 4 jest poświęcony szyfrowi Salsa20. Szyfr ten został zaprojektowany przez Daniela Bernsteina i jest jednym z szyfrów zgłoszonych na europejski konkurs eStream. Szyfr ten składa się z 20 identycznych rund. Ma on dwie wersje w zależności od długości klucza (128/256 bitów). Każda z nich stosuje trzy podstawowe operacje: dodawanie, xor i rotacje (w skrócie ARX od angielskiego Add, Rotate, Xor). W pracy przedstawiono szczegóły kodowania podstawowych operacji wraz z kodowaniem innym pomocniczych przekształceń zastosowanych w szyfrze. Eksperymenty pokazały, że szyfr Salsa20/2 (tzn. szyfr zredukowany do 2 rund) jest łatwy do złamania. Najlepszym uzyskanym przez autorkę rezultatem jest złamanie szyfru Salsa20/4 (szyfr zredukowany do 4 rund) z 128-bitowym kluczem. Jest to znowu atak probabilistyczny, w którym część 68 bitów jest ustalona i znana. Eksperymenty potwierdzają fakt, że Salsa20 jest odporna na kryptoanalizę z SAT solverami.

Tematem rozdziału 5 jest szyfr AES, który jest aktualnym międzynarodowym standardem szyfrowania. Struktura tego szyfru jest oparta na klasycznej sieci Shannona. AES używa kilkunastu jednorodnych rund. Liczba rund zależy od wersji szyfru. Każda runda jest zbudowana z czterech podsta-

wowych operacji: przekształceniu `SubBytes`, przesuwania ciągów binarnych `ShiftRow`, mieszania bajtów `MixColumn` oraz dodawania `XOR` dwóch ciągów binarnych. Głównym wezwaniem tutaj było przetłumaczenie powyższych operacji na język SAT solverów. Część eksperymentalna tego rozdziału wykorzystuje sześć różnych wersji SAT solverów. Testy wykonane dla pojedynczej rundy szyfru AES pokazują, że żadna z wersji solvera nie jest wstanie znaleźć klucza kryptograficznego. Solvery generują poprawne rozwiązania w przypadku, kiedy część bits klucza jest ustalona i znana. Najlepszy rezultat to określenie brakujących 112 bitów klucza, gdy znamy 16 pierwszych bitów klucza kryptograficznego.

Uwagi Edytorskie

Struktura pracy jest przejrzysta, a tekst czyta się łatwo. Z braku dobrego polskiego równoważnika dla nazwy “solver”, autorka używa oryginału angielskiego. Jest to zgodne z powszechnym trendem i nie można mieć tutaj większych zastrzeżeń. Tak na marginesie, byłoby chyba lepiej użyć “solwer”, jako wersję zgodną z polską fonetyką. Na rysunku 4.3 tekst jest nieczytelny – tło w głównym prostokącie jest zbyt ciemne. Można też zauważyć of czasu do czasu pojawiające się literówki.

Podsumowanie

Kryptoanaliza jest bardzo ważną częścią kryptologii i wysoko ceniona przez społeczność akademicką. Rozprawa przedstawia wyniki kryptoanalizy z użyciem SAT solverów. Sam tekst pracy nie pozwala docenić wysiłku autorki niezbędnego do przełożenia początkowych koncepcji ataków na ich implementacje, gdzie dbałość o szczegóły jest koniecznością. Wyniki badań są opublikowane w dwóch międzynarodowych konferencjach naukowych i dalsze dwie publikacje są w przygotowaniu. Oceniam niniejsza rozprawę pozytywnie i stwierdzam, że spełnia ona wymogi stawiane rozprawom doktorskim. Wnioskuję, zatem do Rady Dyscypliny Informatyki Technicznej i Telekomunikacji Szkoły Głównej Gospodarstwa Wiejskiego o przyjęcie rozprawy i dopuszczenie mgr Sylwii Stachowiak do dalszych etapów przewodu doktorskiego.

Podpis cyfrowy Certum Asseco Data Systems

Józef Pieprzyk
Data 61, CSIRO
Sydney, Australia