dr hab. Marek Klonowski
prof. ndzw. PWr
++48 692 842 272
Marek.Klonowski@pwr.edu.pl

Wrocław, 20.10.2019

Recenzja rozprawy doktorskiej Pana mgra Ashutosha Dhara Dwivediego

Niniejszym wnoszę o przyjęcie rozprawy i dopuszczenie Pana mgra Ashutosha Dhara Dwivediego do dalszych etapów przewodu doktorskiego.

Tematyka i struktura pracy

Głównym tematem rozprawy jest kryptoanaliza protokołów szyfrowania, ze szczególnym uwzględnieniem algorytmów dedykowanych urządzeniom o ograniczonych zasobach.

Rozdział pierwszy w głównej części stanowi bardzo ogóle wprowadzenie w tematykę wybranych zagadnień kryptografii.

Rozdział drugi, podobnie jak poprzedni, nie zawiera oryginalnych wyników a jedynie bardziej szczegółowy przegląd technik współczesnej kryptoanalizy.

Rozdział trzeci przedstawia oryginalne wyniki, których współautorem jest Doktorant, a które dotyczą kryptoanalizy szyfru blokowego Scream (uczestnik drugiego etapu konkurs CESAR). Użyto metod kryptoanalizy różnicowej oraz linowej a także ich rozwinięć, które zaowocowały między innymi atakiem na wersję protokołu ograniczoną do 5 rund. Atak wymaga dość sporej liczby kryptogramów. Zaproponowano także atak na 11 rundową wersję protokołu Scream, która zakłada jednak model bardzo silnego adwersarza. Zaprezentowane ataki mają znaczenie głównie teoretyczne, bo sprowadzają się do wykazania przewagi adwersarza w przypadku mocno zredukowanych wersji protokołów. Ponadto sama przewaga jaką adwersarz zdobywa we wskazanych atakach jest w praktyce niezmiernie mała. Same wyniki są powiązane z rezultatami prac opublikowanymi w *Information Processing Letters* oraz na konferencji SECRYPT.

Rozdział czwarty dotyczy kryptoanalizy szyfrów typu ARX (czyli opartych o dodawanie modularne, rotację oraz operację xor). Autor przedstawia pewne ogóle rozważania a potem stosuje je do protokołów SPECK oraz LEA.

Rozdział ten jest najobszerniejszy i zapewne najistotniejszy w całej rozprawie. Zawiera on między innymi nową metodę wyznaczania ścieżki różnicowej opartej o zmodyfikowaną heurystykę *Nested Monte-Carlo search*. Metoda ta zostaje w dalszej części wzbogacona o technikę *częściowych tabel różnicowych* (pDDT), będącą adaptacją wyników innych autorów. W kolejnych krokach zaprezentowane zostało wzbogacenie tej metody o (także znane) podejście oparte o łącznie ścieżek. Zaproponowane podejście zaowocowało licznymi wariantami ataków na różne zredukowane wersje protokołów SPEC oraz LEA. Wyniki uzyskane nową metodą są porównywalne do tych uzyskanych za pomocą innych technik i podobnie jak inne przedstawione w dysertacji ataki mają (jak dotąd) znaczenie głównie teoretyczne ze względu na silnie założenia dotyczące adwersarza jak też bardzo ograniczoną przewagę jaką ataki dają adwersarzowi.

Wyniki tego rozdziału oparte zostały oparte o publikacje w *IEEE Access* oraz *International Journal of Electonics and Telecommunications*.

Rozdział piąty bardzo skrótowo przedstawia kryptoanalizę szyfru ASCON opartą o redukcję do problemu spełnialności. Dodajmy, że atakowany szyfr to zwycięzca kategorii *lightweight applications* w międzynarodowym konkursie CESAR.

Zaprezentowana wersja ataku dotyczy protokołu zredukowanego jedynie do dwóch rund, co sugeruje, że takie podejście do kryptoanalizy ASCON nie jest efektywne. Niewątpliwą zaletą tego typu ataków jest mała wymagana pamięć potrzebna do jego przeprowadzenia oraz stosunkowo mała (w podrównaniu z klasycznymi metodami kryptoanalizy) ilość potrzebnego materiału kryptograficznego. Piąty rozdział oparty jest o wyniki z konferencji SECRYPT.

Rozprawa zawiera także lapidarne zakończenie, krótki apendyks przedstawiający szczegóły jednej z omawianych technik oraz obszerną bibliografię.

Forma

Rozprawa jest napisana w języku angielskim. W mojej ocenie strona językowa stoi na dobrym poziomie. Można znaleźć pewne niezręczności językowe, choć nie wpływają one na zrozumienie tekstu.

Struktura pracy jest przejrzysta a prowadzona narracja w pełni logiczna. Na szczególne uznanie zasługują licznie, bardzo dobrze skomponowane schematy przedstawiające konkretne protokoły.

Ocena wyników rozprawy

Bez wątpienia przedstawione wyniki uzasadniają przyznanie Panu Dwivediemu stopnia naukowego doktora.

Najważniejszym rezultatem rozprawy są niewątpliwie wyniki zamieszczone w rozdziale czwartym, które dotyczą znajdowania ścieżek różnicowych w szyfrach typu ARX. Samo podejście ukierunkowane na przyspieszenie wyszukiwania ścieżek o dużej wadze wymagało pewnej pomysłowości i wyjścia poza powszechnie stosowane schematy stosowane we współczesnej kryptoanalizie. Brakuje tu nieco szerszej dyskusji uzasadniającej właśnie takie podejście do poszukiwania ścieżek o największej wadze. Metoda NMCS, choć intuicyjna, wydaje się być jednym z wielu możliwych podejść. Być może jeszcze lepszą techniką byłoby zastosowanie heurystyki mniej zachłannej? Mimo, że sam pomysł nie jest nowy, uwagę zwraca też efektywne podejście oparte o łączenie ścieżek (4.7.1). Zaproponowane w rozdziale czwartym metody, wydaje się, mają szansę być wykorzystane w przypadku innych schematów, w szczególności opartych o paradygmat ARX.

Wyniki rozdziału trzeciego wydają się mieć mniejsze znaczenie naukowe. W zdecydowanej większości ograniczają się one do zastosowania standardowych narzędzi do konkretnych szyfrów. Do tego, w wyniku przeprowadzonej analizy nie uzyskano żadnych spektakularnych rezultatów o praktycznym znaczeniu. Rezultaty te jednak zasługują na docenienie. Przeprowadzenie takiej analizy jest istotne, bo stanowi ona pewien argument za stosowaniem właśnie tego szyfru i jest ona przyczynkiem do jego ogólnej weryfikacji. Co więcej trzeba zaznaczyć, że przeprowadzenie takiej analizy wymaga bardzo dużej wiedzy na temat nowoczesnych technik kryptoanalitycznych a sama analiza protokołów oparta została o liczne, zróżnicowane metody.

Wyniki rozdziału piątego, czyli kryptoanaliza szyfru ASCON oparta o redukcję do problemu spełnialności, także jest powtórzeniem znanego podejścia. Prezentacji wyników w tym rozdziale można postawić zarzut dotyczący skrótowości przedstawionego rozumowania. Opis ataku jest nieco zbyt ubogi a rezultaty zostały wyeksponowane w niejasny sposób. Byłoby dobrze, gdyby Autor przestawił szczegółową kryptoanalizę dla przykładowej instancji problemu (oczywiście ze zredukowaną liczbą rund). Prezentacja w rozdziale piątym odstaje od standardów stosowanych wcześniej. Zwraca uwagę brak szerszego podsumowania podobnego do wcześniejszych rozdziałów.

Reasumując, mimo że przestawione wyniki nie zakończyły się żadnym spektakularnym sukcesem a całość wyników doprowadziła jedynie do wskazania, że możliwe są skuteczne ataki na algorytmy o mocno zredukowanej liczbie rund, **znaczenie wyników oceniać należy wysoko**. Potwierdza to niejako liczba cytowań prac Doktoranta – ponad 90 (wg Google Scholar) bardzo duża jak na tę dzie-

dzinę i czas w jakim wyniki zostały opublikowane. Podkreślmy, że wyniki te były też cytowane przez naukowców spoza kręgu współautorów Doktoranta.

Warto także nadmienić, że badania prowadzone przez Autora dotyczą szyfrów, które zdobyły pewien rozgłos w międzynarodowych konkursach i zostały wyłonione przez środowisko badawczy jako trudne do złamania. Wynika z tego, że zadanie Autora było bardzo trudne, gdyż atakowane algorytmy zostały zaprojektowane przez świetnych i doświadczonych naukowców. Warto tu też z uznaniem odnotować, że prowadzone badania ściśle wpisują się w główny nurt badań kryptoanalitycznych i odnoszą się do bardzo aktualnych i ważnych problemów. Nie są to zatem badania niszowe, dotyczące algorytmów bez istotnego znaczenia praktycznego. Co więcej dziedzina ta wymaga dość specyficznego podejścia badawczego opartego o bardzo głębokie zrozumienie współczesnych szyfrów oraz bardzo precyzyjne użycie subtelnych metod badawczych.

Zaprezentowane wyniki są oparte na publikacjach m.in. w *IEEE Access*, *IPL* oraz na konferencjach SECRYPT. Są to dobre wydawnictwa międzynarodowe o ustalonej międzynarodowej pozycji, choć spoza światowej czołówki.

Uwagi krytyczne

Nie widzę żadnych wad rozprawy, które zmuszałyby mnie prosić o jej korektę. Mimo to stwierdzić trzeba, że rozprawa nie jest wolna od umiarkowanie istotnych wad oraz drobnych usterek.

- W wielu miejscach Autor zamienne stosuje losową wartość z jej wartością oczekiwaną (m.in. rozważania ze str. 43, str. 48, str. 52). Podobnie w rozdziale 3.6.1 mamy powołanie się na tzw. *paradoks urodzinowy* bez określenia, czy postulowana własność zachodzi z wysokim prawdopodobieństwem dla określonej liczby par tekst jawny-kryptogram, czy może jest to wartość oczekiwana liczby par, przy której następuje tzw. kolizja. W tym przypadku brakuje też precyzyjnie określonych stałych, co ma znaczący wpływ na to kiedy przedstawiony atak ma jeszcze sens, a kiedy jego efekt jest mniej korzystny niż spodziewane rezultaty stosowania trywialnego podejścia opartego o systematyczne przeszukiwanie przestrzeni kluczy. W pewnych miejscach brakuje także dyskusji uzasadniającej, że zdarzenia są stochastycznie niezależne. Ma się jednak wrażenie, że w opisanych przypadkach podejście takie nie doprowadziło do zasadniczych błędów a rozumowania pozostają poprawne. Dodajmy również, że takie podejście można znaleźć w wielu pracach z kryptografii, także bardzo uznanych autorów.

- Opis badań rozdziału piątego jest zbyt skrótowy. Trudno jest zrozumieć szczegóły przeprowadzonych ataków. Brakuje też lepszej prezentacji podsumowującej rezultatów ataków.

- Opisy w rozdziałach pierwszym i drugim są w wielu miejscach nieco nieprecyzyjne (np. paragraf *Amount of Secrecy* na str. 22, *Unkeyrd algorithm* na str. 24 czy próba formalizacji sukcesu ataku str. 30). Sytuacja taka jest jednak do zaakceptowania biorąc pod uwagę wstępny charakter rozważań w początkowych częściach dysertacji.

- Nieco bardziej razi nieprecyzyjna Definicja 1 (str. 26), czy zbyt skrótowy opis ataku w rozdziale 3.5.1.

Można wymienić także kilka **drobnych usterek**, które jednak **nie wpływają na ogólną ocenę rozprawy**. Oto **niektóre** z nich:

- Bibliografia zawiera dość liczne niekonsekwencje i braki. Poszczególne pozycje napisane są w różnych stylach. Nieporozumieniem wydaje się na przykład opis bibliograficzny pozycji [30].

- Mimo, że ogólnie praca napisana jest starannie, znaleźć można literówki i drobne błędy typograficzne oraz językowe.

- Brakuje odnośników bibliograficznych do niektórych klasycznych konstrukcji w rozdziałach wstępnych. Np. do opisu schematu ś.p. Horsta Feistela. Podobnie nie znajdziemy odniesienia do paradoksu urodzinowego (str. 53) oraz kilku innych mechanizmów przywołanych w rozdziale pierwszym i drugim.

- Konkluzje niektórych analiz sugerują bezpieczeństwo badanych protokołów, podczas gdy w rzeczywistości wykazana została jedynie odporność na konkretne rodziny ataków przeprowadzonych w określony sposób.

- Pewne opisy zdają się być zbyteczne. Na przykład taksonomia wprowadzona w rozdziale 1.5.1 zasadniczo nie jest używana w dalszej części pracy.

- Str. 24: argumentacja łącząca istnienie klucza i odwracalność przekształcenia wydaje się być chybiona.

- W taksonomii ataków w 1.5.2 nie jest jasne, kiedy adwersarz ma do dyspozycji nieograniczony czas. Opisy poszczególnych klas zdają się być niespójne.

- Str. 46: jest $C(r)$ zamiast C_r.

- Str. 59: podpis pod rysunkiem 4.3: jest i a powinno być k_i?

- Str. 62, początek 4.5.1: jest *root* powinno być *path*?

- Niejasny opis z 1.6.3. Wartość 2^{k-1} jest oczywiście średnią liczbą prób potrzebną do znalezienia klucza naiwnym podejściem. Jest to zatem co najwyżej ograniczenie dolne na bezpieczeństwo w praktyce.

Uwagi końcowe i podsumowanie

Kilka z przedstawionych rezultatów stanowi widoczny wkład w prowadzone na świecie badania nad odpornością protokołów szyfrowania. Metodologia jest poprawna, przedstawione rozumowania świadczą o opanowaniu przez Doktoranta zaawansowanych metod nowoczesnej kryptoanalizy a niektóre z nich wymagały twórczego podejścia i pomysłowości przy osiąganiu celów naukowych.

Bardzo dobre wrażenie robi również fakt, że prace Pana Dwivediego (łącznie z tymi spoza rozprawy) były cytowane już ponad 90 razy wg. Google Scholar, także przez świetnych naukowców spoza grona współautorów Doktoranta.

Można więc uznać, że wyniki Pana Dwivediego są istotnym głosem w ważnej dyskusji na temat bezpieczeństwa protokołów, które są (lub mogą być) używane w praktyce.

Reasumując, rezultaty stoją na dobrym poziomi według wysokich standardów międzynarodowych. Innymi słowy rozprawa ta mogłaby być z sukcesem przedstawiona jako doktorat na każdym dobrym europejskim uniwersytecie. W szczególności rozprawa ta **w pełni spełnia ustawowe i zwyczajowe wymagania do nadania stopnia doktora**.