dr hab. inż. Andrzej Paszkiewicz, prof. WAT

Instytut Matematyki i Kryptologii

Wydział Cybernetyki

ul. gen. Witolda Urbanowicza 2

00-908 Warszawa

Warszawa 28 marca 2018 r.

RECENZJA ROZPRAWY DOKTORSKIEJ

Pana mgr inż. Michała Strausa

pt. „Kryptoanaliza funkcji gąbkowej Keccak"

1. Uwagi ogólne o tematyce pracy i jej celowości

Przedłożona rozprawa stanowi liczące około 140 stron dzieło, poświęcone zagadnieniu kryptoanalizy funkcji skrótu SHA-3 znanej też pod nazwą Keccak. Funkcje skrótu wykorzystywane są jako element wielu protokołów realizowanych na bazie kryptografii, najczęściej do podpisu cyfrowego, uwierzytelniania danych czy przechowywania odcisków haseł używanych przez użytkowników systemów komputerowych. Pierwowzorem funkcji skrótu są, wykorzystywane wcześniej w telekomunikacji i informatyce sumy kontrolne, służące do badania integralności pliku przechowywanego w komputerze, czy też integralności transmitowanej wiadomości. Niejawnie też funkcje skrótu występują w teorii kodowania. Funkcja skrótu jest odwzorowaniem informacji, której cyfrowy odpowiednik może posiadać dowolną długość w bitach, stąd też dla wielu wiadomości skrót będzie taki sam. Sytuację, w której dwie wiadomości mają ten sam skrót nazywamy kolizją. Dobra funkcja skrótu cechuje się tym, że dla zbioru wszystkich wiadomości o ustalonym rozmiarze częstość pojawiania się różnych skrótów powinna mieć rozkład równomierny. Z drugiej strony też funkcja skrótu powinna cechować się dużą wrażliwością na zmianę wartości informacji podlegającej skracaniu, tzn. zmiana choćby jednego bitu informacji powinna powodować zmianę około połowy bitów skrótu. Stąd też skonstruowanie funkcji skrótu, która spełniałaby choćby tylko przedstawione wcześniej dwa warunki jest zadaniem

trudnym. Stosowane wcześniej funkcje skrótu takie jak SHA-1, rodzina SHA-2 czy MD5 wykazały wiele słabości w konsekwencji czego Amerykański Instytut ds. Standardów i Technologii (NIST) ogłosił konkurs na nową funkcję skrótu, która nie miałaby ujawnionych wad swoich poprzedniczek. W wyniku konkursu wyłoniona została i ogłoszona jako nowy standard SHA-3 całkowicie nowa propozycja oparta na wcześniej nie znanej architekturze gąbki (sponge). Skojarzenie z gąbką jest bardzo trafne, bowiem w trakcie tworzenia skrótu mamy do czynienia z fazą „zasysania" informacji wejściowych a następnie „wyciskania" z nich skrótu.

Architektura gąbki stwarza możliwość dość szerokiego użycia jej w innych zastosowaniach niż projektowanie funkcji skrótu - np. do konstrukcji szyfrów strumieniowych czy do do konstrukcji algorytmów szyfrowania z uwierzytelnianiem. Zauważyli to także twórcy Keccaka proponując nowy szyfr z uwierzytelnianiem o nazwie Keyak.

Od czasu konkursu na Zaawansowany Standard Szyfrowania AES, diametralnie zmieniło się podejście do projektowania szyfrów do użytku publicznego. Zgłaszane w sposób publiczny propozycje podlegają analizie i ocenie w środowiskach akademickich i firmowych. Podejście takie zaowocowało niebywałym rozwojem technik kryptoanalizy i powstaniem nowych narzędzi do badania jakości rozwiązań kryptograficznych. Jednym z nich jest nowy, interesujący typ ataku na szeroką klasę szyfrów symetrycznych, opracowany przez I. Dinura i A. Shamira w 2008 roku, zwany atakiem kostkami (cube attack). Jest to atak typu algebraicznego, który najogólniej mówiąc, umożliwia wykrycie tych „wyjść" szyfrogramu, które są opisane wielomianami niskiego stopnia względem bitów klucza i szyfrowanej wiadomości. Przy zredukowanej liczbie rund szyfru pozwala to na całkowite lub częściowe odzyskanie klucza. Autor przedłożonej pracy zajął się udoskonaleniem ataku kostkami pod kątem przeprowadzenia go w odniesieniu do różnych konfiguracji algorytmu Keccak.

Podjęcie się przez Autora zadania kryptoanalizy funkcji gąbkowej zbiegło się z pracami nad normalizacją nowego standardu funkcji skrótu SHA-3, opartego na strukturze gąbki. Można więc powiedzieć, że praca wpasowuje się we współczesny nurt badań naukowych nad jakością i trwałością propozycji tego standardu, który w założeniach powinien cechować się dużą odpornością na wszelkie manipulacje. Praca posiada także ogólny walor, rozpatruje bowiem funkcję gąbki nie tylko w odniesieniu do funkcji skrótu ale w szerszym rozumieniu – jako prymityw kryptograficzny, który może być wykorzystany do konstrukcji stosunkowo szerokiej klasy szyfrów.

2. Układ i struktura pracy, cel i teza rozprawy

Praca składa się z dziesięciu rozdziałów nie licząc wstępu i podsumowania, zawiera spis treści, streszczenie po polsku i angielsku, wykaz stosowanych oznaczeń. Spis literatury liczy 78 pozycji dobrze skorelowanych z tematem pracy i mających swoje odniesienia w tekście pracy. Cztery spośród cytowanych publikacji stanowią liczące się prace, autora niniejszej

rozprawy. Efekty pracy syntetycznie podsumowano w dziewięciu załącznikach, zawierających odpowiednio: wyniki ataku kostkami na pięć rund algorytmu Keccak działającego w trybie MAC, wyniki ataku na 6 rund algorytm Keccak, działającego w trybie strumieniowym, wyniki ataku kostkami na permutację na algorytm Keccak-f[400], Opis przeprowadzonych symulacji względem teoretycznego ataku na 6 i 7 rund algorytmu Keccak w trybie MAC, wyniki ataku z bocznym kanałem, wyniki ataku sumacyjnego i wyniki analizy sumacyjnej. Pracę ilustruje 30 rysunków ułatwiających rozumienie omawianych treści i interpretację uzyskanych wyników. Kolejne rozdziały pracy to:

I. Kryptograficzne funkcje skrótu. Podano tu klasyfikację funkcji skrótu i opisano wymagania jakie muszą one spełniać pod względem bezpieczeństwa.
II. Keccak. Przedstawiono szczegóły funkcji Keccak i pokazano jak można tę funkcję wykorzystać jako szyfr strumieniowy oraz generator kodu uwierzytelniania wiadomości.
III. Keccak jako podstawa szyfru z uwierzytelnieniem – algorytm Keyak. Znalazł się tu opis szyfru Keyak, wyprowadzonego z algorytmu Keccak, konstrukcja DuplexWrap oraz KeyakLines.
IV. Atak kostkami. Omówiono istotę ataku kostkami wraz z podaniem przykładu.
V. Atak kostkami na algorytm Keccak. Rozdział prezentuje oryginalne pomysły przeprowadzenia ataku na odzyskanie klucza dla 5 rundowego algorytmu działającego w trybie MAC i odzyskanie klucza dla algorytmu działającego w trybie strumieniowym po 6 rundach.
VI. Przewidywanie stanu wyjściowego algorytmu Keccak działającego w trybie z kluczem.
VII. Odzyskiwanie klucza w trybie dziel i zwyciężaj dla algorytmu Keccak i Keyak. Przedstawiono ataki na 6 i 7 rund algorytmu Keyak przy pomocy metody *dziel i zwyciężaj*.
VIII. Wykorzystanie ataku kostkami w atakach bocznym kanałem. Rozważane są ataki typu side channel w połączeniu z atakiem kostkami na algorytm Keccak.
IX. Atak sumacyjny. Zawiera przykład ataku na szyfr Square umożliwiający odzyskanie klucza dla 4 rund.
X. Atak sumacyjny zorientowany bitowo wobec algorytmu Keccak. Rozwinięcie ataku sumacyjnego do postaci zorientowanej bitowo pozwalające uzyskać charakterystykę sumacyjną dla 3 rund i jego rozszerzenie do 4 rund.

2.1. Cel rozprawy:

Przeprowadzenie kryptoanalizy funkcji gąbkowej Keccak i wyznaczenie poziomu jej bezpieczeństwa.

2.2. Tezy rozprawy:

- **Wykorzystanie strukturalnych i algebraicznych własności permutacji Keccak-f pozwala uzyskać lepsze wyniki niż klasyczny atak kostkami.**
- **Specyfika wybranych trybów działania funkcji gąbkowej (np. tryb szyfru strumieniowego, tryb szyfrowania z uwierzytelnianiem) poszerza możliwości kryptoanalizy w porównaniu do kryptoanalizy funkcji skrótu Keccak (SHA-3).**
- **Atak sumacyjny zorientowany bitowo pozwala uzyskać istotnie lepsze rezultaty niż podejście oparte na analizie całych słów.**

3. Mankamenty i błędy dostrzeżone w rozprawie

Przedłożona praca prezentuje dojrzały poziom naukowy i inżynierski, jako że istotną jej część stanowią wyniki uzyskane za pomocą doświadczeń z wykorzystaniem techniki komputerowej. Dotyczy to głównie wyznaczonych w zależności od rodzaju ataku „superwielomianów". Na pewno byłoby rzeczą korzystną zawarcie w pracy informacji (choćby w postaci wzmianki) o tym, jakiego typu sprzęt komputerowy został wykorzystany do wyznaczania kostek, w jakim języku programowania zostały napisane odpowiednie programy komputerowe oraz ile czasu zajęło Autorowi rozprawy wyznaczenie wyników zebranych w tabelach A, B i C zawartych w załącznikach. Podanie takiej informacji byłoby cenne z punktu widzenia kontynuatorów przeprowadzonych ataków, którzy chcieliby je ulepszać i móc porównać z wynikami własnych implementacji, traktując wyniki przedłożonej pracy jako punkt wyjścia lub check point w odniesieniu do własnych doświadczeń. Każdy spośród przedstawionych przez Autora ataków został opisany w sposób wystarczający do zrozumienia jego istoty, jednak znowu brakuje odniesienia do szczegółów implementacyjnych. Z drugiej strony znalazły się w pracy pewne elementy, moim zdaniem, nadmiarowe, jak np. pseudokod pojedynczej rundy permutacji Keccak-f (str. 44) czy szczegółowe wyprowadzenie znanego wzoru na prawdopodobieństwo kolizji (str. 34, 35 i 36) w dodatku zawierające błąd w przedstawieniu funkcji eksponent w postaci szeregu Maclaurina (wzór przybliżony jest poprawny). Szkoda również, że w pracy jedynie w sposób szkicowy opisano metodę etapowego znajdowania klucza z wykorzystaniem zasady „dziel i zwyciężaj" – rozdział 7. Innym, choć niezbyt może istotnym mankamentem przedłożonej pracy, jest fakt, że opis istoty tytułowego ataku kostkami wraz z podanym przykładem, znalazł się dopiero na str. 57 i dalszych a więc po połowie podlegającej ocenie części pracy.

Dostrzeżone przeze mnie błędy mają głównie charakter redakcyjny bądź stylistyczny i nie mają wpływu na jakość pracy i uzyskane rezultaty. Niektóre z nich powstały wskutek przeoczenia, które jest naturalną rzeczą, gdy powstaje potrzeba opisania tego co się zrobiło, co nie jest samo w sobie rzeczą pasjonującą. Chciałoby się w tym momencie przypomnieć znany cytat Alberta Einsteina: *„gdy chcesz opisać prawdę, elegancję pozostaw krawcom"*.

4. Podsumowanie

Przedłożona praca ma charakter oryginalny. Autor nie ograniczył się do opisania wyników uzyskanych przez innych ale w sposób twórczy rozwinął i udoskonalił je w oparciu o własne pomysły. Część wyników uzyskanych przez Autora zostało przez niego wcześniej opublikowanych w prestiżowych materiałach konferencyjnych i w „dobrym towarzystwie". W kilku miejscach natrafiłem także na cytowania przez innych autorów opublikowanych przez Doktoranta prac.

Cel rozprawy został osiągnięty a jej tezy doświadczalnie potwierdzone. W istocie Doktorant wykonał postawione sobie zadanie z pewnym nadmiarem.

W świetle obecnych trendów rozwoju techniki w zastosowaniach cywilnych i wojskowych praca posiada charakter użyteczny, o czym napisałem na początku recenzji. Przeprowadzone prace pokazały przydatność metody ataku kostkami i choć nie spowodowały skompromitowania funkcji gąbkowej pod względem jej przydatności w kryptografii, to jednak ukazały, że przy projektowaniu aplikacji kryptograficznych należy być ostrożnym (jak zawsze), w szczególności przy projektowaniu szyfrów symetrycznych. Przy niezbyt ostrożnym podejściu do opracowywania takich szyfrów możemy narazić się na dekonspirację pewnych bitów klucza już po stosunkowo niewielkiej liczbie iteracji (rund). W tej sytuacji atak kostkami powinien być realnie brany pod uwagę jako test, którego przeprowadzenie mogłoby zapobiec uzyskaniu „szewskiego mata" przez kryptoanalityka pragnącego złamać zaprojektowany szyfr oparty na strukturze gąbkowej.

Biorąc pod uwagę powyższe argumenty uważam, że przedłożona praca spełnia wymagania stawiane przed rozprawami doktorskimi w dziedzinie nauk technicznych zgodnie z ustawą z dn. 14 marca 2003 r o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. Nr 65 poz. 595, z późn. zm.) – przed nowelizacją z dn. 1 października 2011 r. Konkludując, pracę oceniam pozytywnie i wnioskuję o dopuszczenie do jej publicznej obrony.

Gadu