Warszawa, 28 lutego 2018r.

prof. UKSW, dr hab. Mirosław Kurkowski
Instytut Informatyki
Uniwersytet kard. St. Wyszyńskiego
w Warszawie

Recenzja rozprawy doktorskiej mgra inż. Michała Strausa
Kryptoanaliza funkcji gąbkowej Keccak
Promotor: prof. IPI PAN, dr hab. Marian Srebrny
Promotor pomocniczy: dr inż. Paweł Morawiecki

Recenzja niniejsza została sporządzona na prośbę Rady Naukowej Instytutu Podstaw Informatyki PAN w Warszawie. Opiniowana rozprawa dotyczy metod kryptoanalizy algorytmu funkcji haszującej SHA-3 - Keccak oraz pochodnych od niej innych algorytmów kryptograficznych. Przewód doktorski prowadzony jest w dziedzinie nauk technicznych, w dyscyplinie naukowej Informatyka.

Wprowadzenie

Społeczeństwa zależą dzisiaj w wielkim stopniu od przetwarzających ogromne ilości informacji komputerów. Dane te przesyła się poprzez sieci komputerowe i przechowuje w bazach danych. Znaczna część tych informacji powinna być odpowiednio chroniona przed niepowołanym dostępem. Potrzeba odpowiedniego zabezpieczania danych była zauważana przez lata równolegle z rozwojem systemów i sieci komputerowych. W tej sytuacji kryptografia była i jest jedynym odpowiednim środkiem, który może zapewnić potrzebną ochronę danych.

Współcześnie stosowane protokoły i systemy kryptograficzne są często strukturami dość złożonymi a jednym z ich kluczowych elementów są funkcje skrótu. Algorytmy te odwzorowują ciąg bitów o dowolnej długości na ciąg (skrót) o niewielkim, określonym i co równie ważne, stałym rozmiarze. Potrzeba zastosowania takich algorytmów pojawiła sie w związku z coraz szybszym przetwarzaniem coraz większych porcji danych. W wielu zastosowaniach dużo zadowalającym a co ważniejsze efektywniejszym podejściem jest zaszyfrowanie małej, zamiast ogromnej porcji danych, która może reprezentować dane stanowiąc swego rodzaju ich „odcisk palca" (ang. fingerprint).

Funkcje skrótu są dzisiaj szeroko stosowane, m. in. stanowią ważny komponent w systemach podpisu cyfrowego, uwierzytelniania i kontroli integralności danych. Kryptograficzne funkcje skrótu muszą oczywiście spełniać określone wymagania w zakresie szeroko pojętego bezpieczeństwa. Warto również podkreślić, że ze względu na wagę ich zastosowań projektowanie funkcji skrótu i badanie ich własności są obecnie bardzo dynamicznym obszarem badawczym. Często rozwiązania, które jeszcze kilka lat temu były uznawane za wiarygodne, bezpieczne i powszechnie stosowane wypierane są przez ich nowe generacje lub całkowicie nowe algorytmy.

Wziąwszy pod uwagę obecny stan nauki w rozważanej dziedzinie oraz najnowsze potrzeby i trendy badawcze mogę stwierdzić, że badanie własności algorytmów kryptograficznych, a zwłaszcza najnowszych funkcji skrótu, w tym uznanej obecnie za standard funkcji haszującej Keccak jest całkowicie uzasadnione i ważne z punktu widzenia bieżących problemów związanych z rozwojem systemów zabezpieczeń w sieciach i innych systemach komputerowych.

Zawartość rozprawy

Przedstawiona do recenzji praca liczy 85 stron, nie licząc stron zawierających spis treści, spisy dodatków, bibliografię oraz Załączniki. W mojej opinii układ rozprawy budzi niewielkie zastrzeżenia związane z moim zdaniem niewłaściwym podziałem prezentowanych treści na rozdziały. Jeden z rozdziałów liczy 18 stron, inny zaś tylko cztery. Rozdziałów jest w sumie 10 i moim zdaniem można było nieco inaczej rozłożyć treści grupując je w nieco większe partie (rozdziały). Zacytowana w pracy literatura przedmiotu liczy 78 pozycji i moim zdaniem jest dobrana odpowiednio na potrzeby zawartych w rozprawie rozważań.

We Wstępie do rozprawy autor określił Cel pracy i hipotezy badawcze:

Celem (...) pracy jest przeprowadzenie kryptoanalizy funkcji gąbkowej Keccak i wyznaczenie jej poziomu wiarygodności (bezpieczeństwa).

W pracy przyjęto (...) hipotezy badawcze:

1. Wykorzystanie strukturalnych i algebraicznych własności permutacji Keccak-f pozwala uzyskać lepsze wyniki niż klasyczny atak kostkami (...).

2. 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).

3. Atak sumacyjny zorientowany bitowo pozwala uzyskać istotnie lepsze rezultaty niż podejście oparte na analizie całych słów.

Pierwsze trzy rozdziały zawierają informacje o badanych algorytmach. W Rozdziale pierwszym autor przedstawił wybrane, ogólne informacje na temat funkcji skrótu. Przedstawiono ich klasyfikacje oraz opisano wymagania bezpieczeństwa jakie muszą one spełniać. Przedstawiono różne konstrukcje funkcji skrótu, w tym miedzy innymi MD5 i SHA-1. Opisano również podstawowe metody ataków na funkcje skrótu. Rozdział drugi przedstawia dokładną specyfikację funkcji Keccak. Przedstawiono szczegółowo wszystkie elementy składowe funkcji. Pokazano również zastosowanie funkcji gąbkowej z kluczem jako: szyfru strumieniowego, szyfru z uwierzytelnianiem i generatora kodu uwierzytelnienia. W rozdziale trzecim opisano opracowany na podstawie algorytmu Keccak szyfr z uwierzytelnianiem Keyak.

Rozdział czwarty omawia jedną z najnowszych obecnie metod kryptoanalitycznych tzw. atak kostkami (ang. cube attack) zaproponowany przez Dinura i Shamira. Wprowadzono podstawowe definicje potrzebne do omówienia schematu ataku. Zaprezentowano i szczegółowo omówiono przykład takiego ataku.

Kolejne rozdziały przedstawiają wyniki badawcze uzyskane przez autora. W Rozdziale piątym opisano autorską metodę kryptoanalizy funkcji gąbkowej Keccak wykorzystującą atak kostkami. Pokazano między innymi procedurę odzyskania klucza dla pięciu rund funkcji działającej w trybie MAC oraz dla sześciu rund dla algorytmu działającego w trybie szyfru strumieniowego. Opisano również odzyskiwanie klucza dla algorytmu Keyak. Rozdział szósty prezentuje analizę algebraicznych właściwości permutacji Keccak-f. Przedstawione są także ataki pozwalające przewidzieć stan wyjściowy dla algorytmu Keccak działającego w różnych trybach z kluczem. W Rozdziale siódmym przedstawiono ataki na sześć i siedem rund funkcji Keccak oraz na siedem rund algorytmu Keyak. W połączeniu z analizą zawartą w poprzednim rozdziale wykorzystano tu metodę „dziel i zwyciężaj". Rozdział ósmy opisuje tzw. ataki bocznym kanałem (ang. side channel). Pokazano jak można zastosować ten typu ataku wobec algorytmu Keccak w połączeniu z atakiem kostkami. W rozdziale dziewiątym opisano podstawy techniki nazywanej atakiem sumacyjnym (ang. integral attack), co wykorzystano w rozdziale dziesiątym, gdzie pokazano jak można przeprowadzić atak sumacyjny zorientowany bitowo wobec algorytmu Keccak.

W Załącznikach przedstawiono pełne wyniki prac opisanych w rozdziałach 5, 6, 7, 8 i 10.

Opinia merytoryczna rozprawy

Jak napisałem wcześniej, układ rozprawy moim zdaniem nie budzi większych zastrzeżeń.

Wstępne części rozprawy wprowadzające podstawowe pojęcia i struktury potrzebne do dalszych rozważań moim zdaniem zostały opracowane dobrze. Uważam, że czytelnik został odpowiednio zaznajomiony z podstawami teoretycznymi oraz obecnym stanem wiedzy w rozważanej tematyce, aby zrozumiale śledzić treści zawarte w rozprawie.

Prowadzone dalej rozważania są przedstawiane zrozumiale i wystarczająco. Za najważniejszy moim zdaniem wynik naukowy przedstawiony w rozprawie uważam atak kostkami na 6-rundowy wariant Keccaka działającego w trybie szyfru strumieniowego. Do klasycznej metody ataku kostkami zostały tutaj dodane wnioski ze strukturalnej i algebraicznej analizy permutacji Keccaka. Innym, równie ważnym wynikiem jest nowy wariant ataku kostkami wykorzystujący paradygmat „dziel i zwyciężaj". Jak zaznaczono w rozprawie podejście to pozwala na teoretyczne ataki na 7mio i 8-rundowe warianty funkcji gąbkowej działającej w trybie szyfru strumieniowego oraz szyfrowania z uwierzytelnianiem algorytmem Keyak. Należy podkreślić, że wyniki te są dzisiaj najlepsze na świecie w tej dziedzinie.

Zaznaczyć również można, że omówione w rozprawie wyniki dotyczące ataku kostkami i jego wariantów zostały przedstawione i opublikowane na prestiżowej konferencji *SHA-3 2014 Workshop* organizowanej przez NIST (National Institute of Standards and Technology) w Stanach Zjednoczonych oraz na konferencji *Eurocrypt* w 2015 roku.

Podsumowując tę część recenzji stwierdzam, że moim zdaniem mgr inż. Michał Straus zrealizował postawiony Cel badawczy i wykazał postawione na początku rozprawy hipotezy.

Uwagi polemiczne i krytyczne

Przedstawione niżej uwagi nie zmniejszają moim zdaniem wartości naukowej rozprawy i nie mają wpływu na pozytywną opinię pracy jako całości.

W Rozdziale trzecim mgr Straus przybliża algorytm szyfrowania z uwierzytelnieniem Keyak, bazujący na permutacji Keccak-f. Z punktu widzenia dalszych rozważań wydaje się, że opis ten jest zbyt szczegółowy, szczególnie, że później do ataków wykorzystywane są tylko podstawowe funkcjonalności szyfru Keyak. W szczególności dla większej czytelności tego fragmentu rozprawy pełna specyfikacja sposobu dopełniania bitów czy kodowania „paczki" kluczy mogłaby zostać pominięta.

W Rozdziale czwartym w przedstawionych tabelach bity stanów numerowane są jedną liczbą (od 1 do 1600). Nie znalazłem wyjaśnienia tej notacji, w całej pracy bity stanu określane są trzema współrzędnymi (trójwymiarowa tablica). Odnośnie użytej notacji i nazewnictwa, uważam za niefortunne tłumaczenie fragmentu stanu określonego po angielsku „sheet" jako „płyta".

W Rozdziale czwartym znajdujemy kluczowe dla dalszych rozważań definicje związane z atakiem kostkami. Niestety definicje te są moim zdaniem wprowadzone niezbyt precyzyjnie. Brak opisu niektórych symboli. Pewne określenia są niejasne.

I tak w Definicjach 2, 3 i 4 czytamy:

Każdy bit wyjściowy kryptosystemu może być przedstawiony za pomocą wielomianu w ciele dwuelementowym GF(2), którego zmiennymi są bity wejściowe. (...) Taki wielomian, oznaczony jako p, może być przedstawiony w następującej postaci:

$$p(x_0, \ldots, x_{n-1}) \equiv t_I \cdot p_{S(I)} + q(x_0, \ldots, x_{n-1}), \qquad (8)$$

gdzie I jest podzbiorem indeksów zmiennych p, $I \subseteq \{0, \ldots, n-1\}$, a n jest liczbą argumentów p.

Definicja 3. Superwielomianem nazwano $p_{S(I)}$, który nie ma wspólnej zmiennej z jednomianem t_I.

Definicja 4. Maxtermem nazwano taki jednomian t_I, dla którego stopień superwielomianu jest równy 1, $deg(p_{S(I)}) = 1$. Pozostała część wielomianu p, oznaczona jako q, nie zawiera jednomianu równego t_I.

Określenia te są kluczowe dla całej rozprawy. Sposób ich przedstawienia ma moim zdaniem sporo mankamentów. Nie przedyskutowano, czy takie przedstawienie wielomianu p jest jednoznaczne. Nie wiadomo w jaki sposób można je uzyskać i czy jest to konieczne dla prowadzenia ataku? Brak zmiennych dla wielomianów t_I i $p_{S(I)}$ we wzorze *(8)* może wprowadzać w błąd czym są te czynniki. Nie znalazłem określenia co to jest $S(I)$. Trzeba się domyślać, że $I \cap S(I) = \varnothing$, ale czy tylko o to chodzi?. Definicja 3 jest nieco dziwna. Przy zastosowanych oznaczeniach i strukturach nigdy $p_{S(I)}$ nie ma wspólnej zmiennej z t_I (oczywiście z dokładnością do faktu, że nad $GF(2)$ dla dowolnej zmiennej jest $x^2=x$). Sytuację ratuje tutaj nieco bezpośrednie odwołanie do artykułu Dinura i Shamira, z którego konstrukcje te są wzięte i możliwość doczytania i lepszego zrozumienia tego materiału oraz przedstawienie dalej odpowiednich przykładów. Wydaje się jednak, że ten fragment powinien być lepiej opracowany.

W Rozdziale szóstym zaprezentowany jest atak fałszujący kod MAC dla 8-rund. Autor użył jednak dość długiego, bo mającego 256 bitów kodu, niespotykanego raczej w praktycznych rozwiązaniach. Powinno zostać chyba zaznaczone, że atak ten ma raczej charakter teoretyczny.

W Rozdziale dotyczącym ataku sumacyjnego zabrakło mi podsumowania opisującego przedstawiony atak w nieco szerszym kontekście. Autor pracy zaznacza w podsumowaniu rozprawy, że hipoteza dotycząca tego ataku okazała się nieprawdziwa lecz brakuje głębszej analizy dlaczego tego typu atak zawiódł (tylko 4 rundy) mimo sukcesów z innymi szyframi (np. szyfr PRESENT). W szczególności wnikliwiej powinna zostać przeanalizowana dyfuzja w pierwszych kilku rundach (zarówno jakościowa jak i ilościowa analiza).

W Rysunkach 21 i 22 w podrozdziale 9.2.1 użyłbym raczej określenia „Atak typu Square".

Ciekawym zastosowaniem analizy kostkowej jest przedstawiony atak z kanałem bocznym (ang. side-channel attack). To co jednak budzi pewną wątpliwość to do jakiego stopnia opisany atak jest praktyczny. Atak został tylko zasymulowany, co przy tego rodzaju analizie ma swoje oczywiste ograniczenia. W szczególności niejasne jest czy atakujący kiedykolwiek będzie miał dostęp do tak wielu wywołań funkcji szyfrującej (w tym scenariuszu zwykle działającym na małym urządzeniu typu o ograniczonych zasobach).

W kilkunastu miejscach rozprawy znaleźć można określenia lub stwierdzenia moim zdaniem czasem zbyt kolokwialne lub nieprecyzyjne jak na rozprawę doktorską. Zwracam uwagę na poniższe przykłady:

- str. 13 – *kryptologia (...) jako (...) dziedzina wiedzy*,
- str. 13 – *protokoły (...) są (...) systemami a jednym z kluczowych elementów jest funkcja skrótu*,
- str. 22 – *odnalezienie wiadomości (...) jest niemożliwe w praktyce*,
- str. 23 – *odnajdywanie kolizji jest niemożliwe w praktyce*,
- str. 32 – *nie zaleca się stosowania skrótu SHA-1, ponieważ nie jest już uważany za wiarygodny*,
- str. 40 – *cała ta praca (...) stanowi formalną analizę i dowód bezpieczeństwa funkcji gąbkowej*,
- str. 41 – *wyjście funkcji gąbkowej*,
- str. 41 – *Bezpieczeństwo schematów kryptograficznych zazwyczaj oparte jest na złożoności obliczeniowej*,
- str. 53 i dalej – stosowanie nawiasów klamrowych dla oznaczenia ciągów.

- str. 55 i inne – co to jest *przepływność obiektu*,
- str. 63 i dalej – wyrażenie *stałe, liniowe*, a równanie *stałe, liniowe*,
- str. 71 – *ataki o złożoności praktycznej*,
- str. 78 – *Podrobienie* – co to jest, czy ma coś wspólnego z drobiem, rozdrabnianiem?

Uwagi redakcyjne

Jak każda praca naukowa również recenzowana rozprawa nie jest wolna od niedociągnięć, pomyłek, czy błędów natury redakcyjnej. Trzeba jednak stwierdzić, że rozprawa mgra inż. Michała Strausa zawiera wyjątkowo mało takich pomyłek. Poniżej zamieszczam listę kilku przykładowych pomyłek/błędów:

- str. 26-28 – brak opisu wzorów,
- str. 59 – *skłądnik*,
- str. 64, 68 i dalej – puste fragmenty stron,
- str. 55, 60 i inne – braki interpunkcyjne.

Wniosek końcowy

Przedstawione w recenzowanej rozprawie doktorskiej rozważania związane z metodami kryptoanalizy funkcji Keccak i jej pochodnych dotyczą bieżących, ważnych i interesujących problemów naukowych związanych z konstrukcją i metodami analizy współczesnych systemów kryptograficznych. Rozprawa doktorska mgra inż. Michała Strausa zawiera wiele oryginalnych oraz interesujących wyników. Moje uwagi krytyczne zawarte w recenzji nie zmieniają pozytywnej opinii o rozprawie jako całości.

Biorąc pod uwagę wyniki naukowe przedstawione w recenzowanej rozprawie mgra inż. Michała Strausa stwierdzam, że moim zdaniem, praca ta spełnia wymagania stawiane rozprawom doktorskim przez obowiązującą aktualnie w Polsce Ustawę o Stopniach i Tytule Naukowym. Stawiam zatem wniosek o dopuszczenie mgra inż. Michała Strausa do dalszych etapów przewodu doktorskiego prowadzonego w dziedzinie nauk technicznych w dyscyplinie Informatyka przez Radę Naukową Instytutu Podstaw Informatyki PAN Warszawie.