Poznań, 04.05.2017 r.

Dr hab. inż. Krzysztof Chmiel
Instytut Automatyki i Inżynierii Informatycznej
Politechnika Poznańska

Recenzja rozprawy doktorskiej
pana magistra Przemysława Sokołowskiego
zatytułowanej
„Design and Analysis of Cryptographic Hash Functions"

1. Wstęp

Niniejsza recenzja została opracowana na wniosek Dziekana Wydziału Matematyki i Informatyki Uniwersytetu im. Adama Mickiewicza w Poznaniu, przedstawiony w piśmie z dnia 28.02.2017 r. informującym o powołaniu mnie w dniu 24.02.2017 r. przez Radę Wydziału Matematyki i Informatyki UAM na recenzenta rozprawy doktorskiej pana magistra Przemysława Sokołowskiego zatytułowanej „Design and Analysis of Cryptographic Hash Functions".

2. Struktura rozprawy

Rozprawa napisana jest w języku angielskim, liczy 159 stron i składa się ze streszczenia (w języku polskim i angielskim), podziękowań, deklaracji Autora, siedmiu rozdziałów (numerowanych od 1 do 7), dwóch dodatków (oznaczonych A i B) oraz bibliografii zawierającej 127 pozycji.

Rozdział 1, zatytułowany "Introduction", zawiera ogólny opis przedmiotu rozprawy. Przedstawiono w nim podstawowe własności kryptograficznych funkcji skrótu (podrozdział 1.1) klasyfikację funkcji skrótu (podrozdział 1.2), zastosowania funkcji skrótu (podrozdział 1.3), metody kryptoanalizy (podrozdział 1.4) z podziałem na niezależne od algorytmu (punkt 1.4.1) i zależne od algorytmu (punkt 1.4.2), standardy bezpiecznych algorytmów skrótu (podrozdział 1.5) oraz strukturę rozprawy (podrozdział 1.6). Cel rozprawy nie został sformułowany, ale jest nim zapewne całościowe przedstawienie wyników Autora w zakresie metod analizy kryptograficznych funkcji skrótu oraz wniosków dotyczących zasad ich projektowania.

Rozdział 2, zatytułowany "Cryptographic Hash Functions", poświęcony jest w całości kryptograficznym funkcjom skrótu. Przedstawiono w nim definicję funkcji skrótu i definicje własności kryptograficznych funkcji skrótu (podrozdział 2.1), wykorzystywane architektury funkcji skrótu i metody konstrukcji funkcji kompresji (podrozdział 2.2), jednoblokowe i dwublokowe tryby pracy szyfrów blokowych w funkcjach skrótu (podrozdział 2.3),

porównanie analizy bezpieczeństwa szyfrów blokowych w modelu z tajnym kluczem i jawnym kluczem (podrozdział 2.4), metody analizy funkcji skrótu (podrozdział 2.5) z podziałem na niezależne od algorytmu (punkt 2.5.1) i zależne od algorytmu: analizę różnicową (punkt 2.5.2), analizę rotacyjną (punkt 2.5.3) i analizę przesunięciową (punkt 2.5.4), a także definicję T-funkcji i S-funkcji (punkt 2.5.5).

W rozdziale 3, zatytułowanym "Open Key Differential Analysis for Block Ciphers", zawarto analizę odporności funkcji skrótu wykorzystujących szyfr blokowy na ataki różnicowe w modelu z jawnym kluczem. Przedstawiono w nim wpływ ścieżek różnicowych w modelu ze znanym kluczem na tryby pracy szyfrów blokowych w funkcjach skrótu (podrozdział 3.1), dolne ograniczenie złożoności różnicowego rozróżniacza dla losowych permutacji (podrozdział 3.2), różnicowe ścieżki dla wybranych szyfrów blokowych (podrozdział 3.3) takich jak Crypton, Hierocrypt-3, Square (punkt 3.3.1) i SAFER++ (punkt 3.3.2), a ponadto dla szyfrów Feistela (punkt 3.3.3). Rozdział zamyka podsumowanie z zebraniem wyników w tabeli 3.3 (podrozdział 3.4). Wyniki przedstawione w rozdziale opublikowano w pozycji [109] spisu literatury.

Rozdział 4, zatytułowany "IDEA in Various Hashing Modes", poświęcono analizie bezpieczeństwa trybów pracy szyfru IDEA w funkcjach skrótu. Przedstawiono w nim opis szyfru IDEA (podrozdział 4.1), słabe klucze szyfru IDEA (podrozdział 4.2) z analizą funkcji wewnętrznych szyfru (punkt 4.2.1), klas słabych kluczy (punkt 4.2.2) i klucza zerowego (punkt 4.2.3), proste ataki kolizyjne na 6 wybranych trybów pracy (podrozdział 4.3), ulepszone ataki kolizyjne (podrozdział 4.4) z opisem podstawy ulepszeń (punkt 4.4.1) i samych ataków na 6 uprzednio wybranych trybów pracy (punkt 4.4.2) oraz ataki preobrazowe na te same tryby pracy (podrozdział 4.5). Rozdział kończy podsumowanie z zebraniem wyników w tabeli 4.6 (podrozdział 4.6). Wyniki przedstawione w rozdziale opublikowano w pozycji [125] spisu literatury.

Rozdział 5, zatytułowany "Analysis of Addition-Rotation-XOR Designs", poświęcono kryptoanalizie rotacyjnej struktur ARX i ich rozszerzeń. Przedstawiono w nim własności rotacyjne wielokrotnych dodawań i wielokrotnych odejmowań (podrozdział 5.1), rotacyjne pary z korekcją (podrozdział 5.2) z definicją problemu (punkt 5.2.1) i zastosowaniem dla funkcji dodawania (punkt 5.2.2), analizę rotacyjną funkcji skrótu BMW-512 (podrozdział 5.3) z opisem rotacyjnych własności przekształceń składowych (punkt 5.3.1) i analizą wariantu BMWv1-512 (punkt 5.3.2), ulepszony atak na pełną wersję BMWv1-512 (podrozdział 5.4) z analizą i atakiem na zmodyfikowany wariant BMWv2-512 (punkt 5.4.1), analizę rotacyjną funkcji skrótu SIMD-512 (podrozdział 5.5) z analizą struktury Feistela w SIMD-512 (punkt 5.5.1), analizą uproszczonej wersji SIMD-512 o zredukowanej liczbie rund (punkt 5.5.2) i analizą wersji SIMD-512 o zredukowanej liczbie rund (punkt 5.5.3) oraz analizę przesunięciową funkcji skrótu Shabal (podrozdział 5.6). Rozdział zamyka podsumowanie z zebraniem wyników w tabeli 5.6 (podrozdział 5.7). Wyniki przedstawione w rozdziale opublikowano w pozycji [110] spisu literatury.

Rozdział 6, zatytułowany "Rotational Cryptanalysis and Chained Modular Additions", zawiera wyniki w zakresie kryptoanalizy rotacyjnej łańcuchów dodawań modularnych.

Przedstawiono w nim własności łańcuchów dodawań modularnych (podrozdział 6.1) i ich zastosowanie (podrozdział 6.2) w kryptoanalizie rotacyjnej funkcji skrótu BLAKE2 (punkt 6.2.1), funkcji skrótu Skein (punkt 6.2.2) i rozważanej w rozdziale 5 funkcji skrótu SIMD-512 (punkt 6.2.3). Rozdział zamyka podsumowanie (podrozdział 6.3). Wyniki przedstawione w rozdziale opublikowano w pozycji [65] spisu literatury.

Rozdział 7, zatytułowany "Conclusions" zamyka rozprawę. Przedstawiono w nim podsumowanie wyników Autora opisane w rozdziałach od 3 do 6 (podrozdział 7.1), wskazówki projektowe odnośnie konstrukcji funkcji skrótu (podrozdział 7.2) oraz możliwe kierunki badań w zakresie kryptograficznych funkcji skrótu (podrozdział 7.3).

Załączniki zawierają dowody lematów, przedstawionych w punkcie 2.5.3, o prawdopodobieństwie rotacyjnym operacji przesunięcia, funkcji boolowskiej i mnożenia (dodatek A) oraz opis szyfru mCrypton (dodatek B).

3. Ocena merytoryczna rozprawy

Problematyka recenzowanej rozprawy jest aktualna. Dotyczy badania i konstruowania efektywnych metod analizy kryptograficznej szyfrów blokowych i funkcji skrótu. Wprawdzie idea kryptoanalizy różnicowej przedstawiona została przez E. Bihama oraz A. Shamira podczas konferencji CRYPTO'90, a idea kryptoanalizy liniowej przedstawiona została przez M. Matsui oraz A. Yamagishi podczas konferencji EUROCRYPT'92, ale metody te i ich rozszerzenia, jak np. kryptoanaliza ze skróconymi różnicami, wraz z wprowadzonymi później atakami algebraicznymi, odbiciowymi i rotacyjnymi stanowią główne i wciąż intensywnie rozwijane narzędzia oceny szyfrów i funkcji skrótu. Analizowane są również połączenia powyższych metod w złożony atak, np. różnicowo-algebraiczny czy liniowo-algebraiczny.

Celem rozprawy jest przedstawienie wyników Autora w zakresie metod analizy kryptograficznych funkcji skrótu oraz wniosków dotyczących zasad ich projektowania. Badaniu poddano szyfry Crypton, Hierocrypt-3, Square, SAFER++ i IDEA w modelu z otwartym kluczem oraz funkcje skrótu BMW, SIMD, BLAKE, Skein i Shabal zgłoszone do konkursu na SHA-3, zakończonego w 2012 roku.

Do najważniejszych osiągnięć rozprawy należą:

1. Określenie najlepszych różnicowych ataków kolizyjnych na tryby pracy szyfru blokowego w funkcji kompresji

   Wyniki uzyskane dla 12 trybów jednoblokowych i 4 dwublokowych przedstawiono w tabelach, odpowiednio, 3.1 i 3.2 (str. 44). Rozważono 4 rodzaje ataków kolizyjnych na funkcję kompresji, oznaczane C, PC, SFSC i FSC. Założono, że atakujący może wyznaczyć różnicową ścieżkę dla szyfru o niezerowej różnicy tekstu jawnego, niezerowej różnicy klucza lub niezerowych różnicach tekstu jawnego i klucza. Sposób rozumowania dla modelu z jawnym kluczem przedstawiono na przykładzie jednoblokowego trybu DM (Davies-Meyer).

2. Dowód Lematu 3.1 o dolnej granicy złożoności różnicowego rozróżniacza dla losowej permutacji

W Lemacie 3.1 (str. 45) podano dolną granicę liczby prób dla wyznaczenia różnicowej pary, zgodnej z pewną parą wejście-wyjście skróconych różnic, w przypadku losowej permutacji. Wynik ten jest wykorzystywany do porównań z różnicowymi rozróżniaczami szyfrów, np. w tabeli 3.3 (str. 58). Autor stwierdza, że podobna granica była w literaturze wykorzystywana, np. w pozycji [50] spisu literatury, ale nie został przedstawiony jej formalny dowód.

3. Wyznaczenie różnicowych rozróżniaczy dla szyfrów Crypton, Hierocrypt-3 i Square w modelach ze znanym kluczem i z wybranym kluczem

Szyfry Crypton, Hierocrypt-3 i Square są 128-bitowymi szyframi SP o liczbie rund zależnej od długości klucza. W modelu z tajnym kluczem inni autorzy opublikowali ataki na 8-rundowy Crypton [68], 3.5-rundowy Hierocrypt-3 [8] i 8-rundowy Square [76]. W rozprawie Autor rozważa ataki w modelu z jawnym kluczem. W modelu ze znanym kluczem deklaruje atak o złożoności 2^{48} szyfrowań na 7-rundowy Crypton, 3.5-rundowy Hierocrypt-3 i 7-rundowy Square. W modelu z wybranym kluczem deklaruje atak o złożoności 2^{48} szyfrowań na 8-rundowy Crypton z kluczem 128-bitowym, 9-rundowy Crypton z kluczem 256-bitowym, 4-rundowy Hierocrypt-3 z kluczem 128-bitowym, 4.5-rundowy Hierocrypt-3 z kluczem 256-bitowym oraz 8-rundowy Square. Wykorzystywane w atakach różnicowe ścieżki przedstawiono na rysunkach 3.1, 3.2 i 3.3 (str. 50). Dla losowej permutacji, zgodnie z lematem 3.1, liczba szyfrowań wynosi 2^{61}. Uzyskane wyniki podsumowano w tabeli 3.3 (str. 58). Dla potwierdzenia tych wyników wykonano eksperyment na szyfrze mCrypton [92], opisanym w dodatku B rozprawy, stanowiącym uproszczoną wersję szyfru Crypton.

4. Skonstruowanie ataku typu „rebound" na 6.5-rundowy SAFER++ z kluczem 128-bitowym w modelu z wybranym kluczem

Szyfr SAFER++ jest 128-bitowym szyfrem SP. Wersja z kluczem 128-bitowym ma 7 rund. W literaturze inni autorzy opublikowali atak na 5.5 rund tej wersji [19]. W rozprawie Autor przedstawił atak typu „rebound" na 6.5-rundowy SAFER++ z kluczem 128-bitowym w modelu z wybranym kluczem. Wykorzystywaną w ataku ścieżkę o standardowych różnicach przedstawiono na rysunkach 3.5 i 3.6. W ścieżce tej jest 16 aktywnych S-bloków, co przy założeniu prawdopodobieństwa 2^{-7} aproksymacji S-bloku daje złożoność ataku 2^{112} szyfrowań. Dla losowej permutacji złożoność ataku wynosi 2^{128} szyfrowań. Zgodnie z wiedzą Autora jest to pierwszy atak typu „rebound" o standardowych różnicach.

5. Skonstruowanie ataków kolizyjnych i preobrazowych na tryby pracy szyfru IDEA w funkcji kompresji

Szyfr IDEA jest 64-bitowym szyfrem z kluczem 128-bitowym o 8.5 rundach. W rozprawie przeanalizowano bezpieczeństwo szyfru w następujących trybach: Davies-Meyer, Hirose, Abreast-DM, Tandem-DM, Peyrin et al.(II) oraz MJH-Double. Proste ataki kolizyjne o złożoności 2^1, oparte na wykorzystaniu słabego klucza zerowego szyfru, możliwe są dla trybów Davies-Meyer, Hirose oraz Peyrin et al.(II). Ulepszone ataki kolizyjne, oparte na zerowym kluczu i wykrytej przez Autora własności szyfru nazwanej „almost half-involution", uzyskano dla wszystkich rozważanych trybów. W atakach preobrazowych wykorzystano spostrzeżenie, że przekształcenie szyfru IDEA przy zerowym kluczu jest T-funkcją. Uzyskane wyniki podsumowano w tabeli 4.6 (str. 77).

6. Rozszerzenie kryptoanalizy rotacyjnej na elementarne operacje spoza zestawu operacji ARX (dodawanie arytmetyczne, rotacja, operacja XOR)

Prawdopodobieństwo rotacyjne struktur ARX zależy wyłącznie od dodawań (dla operacji rotacji i XOR jest równe 1). Wyznaczono prawdopodobieństwo rotacyjne dla operacji odejmowania, przesunięć w lewo i w prawo, wykonywanych na odpowiadających sobie bitach funkcji boolowskich sumy, iloczynu i negacji oraz operacji mnożenia (tu występuje niejasność co do autorstwa). Wyniki przedstawiono w lematach 2.1, 2.2, 2.3 i 2.4 (str. 35), a dowody lematów 2.2, 2.3 i 2.4 w dodatku A (str. 139-140). Przedstawiono również prawdopodobieństwo rotacyjne wielokrotnych dodawań, w udowodnionym lemacie 5.1 (str. 82-84), oraz wielokrotnych dodawań i odejmowań, w udowodnionym lemacie 5.2 (str. 84-86).

7. Przedstawienie rozszerzenia kryptoanalizy rotacyjnej na rotacyjne pary z korekcją oraz sposobu obliczania prawdopodobieństwa tych par dla operacji dodawania

Korekcje w kryptoanalizie rotacyjnej stanowią odpowiednik różnic w kryptoanalizie różnicowej. Wykazano, że dla rotacyjnych par z korekcją prawdopodobieństwo rotacyjne operacji rotacji i XOR jest równe 1 (str. 87). W przypadku operacji dodawania arytmetycznego, wykorzystując metodologię S-funkcji, przedstawiono Lemat 5.3 (str. 91), z którego wynika prawdopodobieństwo rotacyjne określone wzorem (5.12). Prawdopodobieństwo rotacyjne struktur ARX zależy więc wyłącznie od prawdopodobieństwa rotacyjnego dodawań, zależnego od wartości korekcji.

8. Wyznaczenie rotacyjnych rozróżniaczy dla funkcji skrótu BMW-512

Funkcja skrótu BMW-512, zgłoszona do konkursu na SHA-3, analizowana jest w rozprawie w dwóch nieznacznie różniących się wariantach, oznaczonych jako BMWv1 i BMWv2. Blok wiadomości i wartości łańcuchowe są rozmiaru 1024-bity. Funkcja kompresji skonstruowana jest z użyciem trzech funkcji składowych f_0, f_1 i f_2 (str. 94-95). W wyniku szczegółowej analizy rotacyjnej funkcji składowych odróżniono warianty BMWv1 i BMWv2 od losowych funkcji, a także przedstawiono ataki rotacyjne na te warianty (str. 95-103). Porównanie rozróżniaczy dla funkcji skrótu BMW-512 przedstawiono w tabeli 5.6 (str. 113).

9. Wyznaczenie rotacyjnych rozróżniaczy dla funkcji skrótu SIMD-512

Funkcję skrótu SIMD-512 zgłoszono do konkursu na SHA-3 w dwóch wariantach: podstawowym (do rundy pierwszej) i zmodyfikowanym (do rundy drugiej). Przedstawione w rozprawie rotacyjne rozróżniacze dotyczą obu wariantów i wyznaczone zostały dla zredukowanej do 24 rund uproszczonej wersji SIMD-512 o zlinearyzowanym algorytmie generacji kluczy (str. 106-107) oraz zredukowanej do 12 rund oryginalnej wersji SIMD-512 (str. 107-109). Porównanie rozróżniaczy dla funkcji skrótu SIMD-512 przedstawiono w tabeli 5.6 (str. 113).

10. Wprowadzenie kryptoanalizy przesunięciowej i wyznaczenie przesunięciowych rozróżniaczy dla funkcji skrótu Shabal

Zaproponowana przez Autora kryptoanaliza przesunięciowa, w odróżnieniu od kryptoanalizy rotacyjnej, oparta jest na przesunięciach, a nie rotacjach. Funkcję skrótu Shabal zakwalifikowano do drugiej rundy konkursu na SHA-3. Jej funkcja kompresji oparta jest na zależnej od klucza permutacji P. W rozprawie wyznaczono prawdopodobieństwo przesunięciowe przekształceń składowych permutacji P (str. 110-112), a w szczególności operacji dodawania, XOR, mnożenia przez 3 i 5, iloczynu logicznego oraz rotacji (Lemat 5.4), operacji aktualizacji zmiennych B_i permutacji P (Lemat 5.5) i operacji mnożenia (Lemat 5.6). Na tej podstawie wyznaczono przesunięciowy rozróżniacz dla permutacji P, lepszy od rozróżniacza rotacyjnego, opublikowanego w pozycji [1] spisu literatury. Porównanie rozróżniaczy dla funkcji skrótu Shabal przedstawiono w tabeli 5.6 (str. 113).

11. Lemat 6.1 o prawdopodobieństwie rotacyjnym łańcuchów dodawań modularnych

W Lemacie 6.1 (str. 118) podano formułę określającą dokładną wartość prawdopodobieństwa rotacyjnego łańcucha dodawań k słów n-bitowych przy rotacji o r bitów. Przedstawiono szczegółowy dowód tego lematu (str. 118-122) i w tabeli 6.1 (str. 123) porównano wartości prawdopodobieństwa obliczone na podstawie lematu 6.1 z wartościami obliczonymi na podstawie twierdzenia 6.1 (str. 116), przytoczonego z pozycji [64] spisu literatury, dla liczby dodawań k-1 od 1 do 8, parametru r rotacji 1 i 2 oraz długości n słowa równej 32 i 64 bity. Wartości prawdopodobieństwa obliczone na podstawie lematu są zdecydowanie mniejsze.

12. Zastosowanie lematu 6.1 do kryptoanalizy rotacyjnej funkcji skrótu BLAKE2

Funkcja skrótu BLAKE2 jest następną wersją funkcji BLAKE zakwalifikowanej do finału konkursu na SHA-3. Funkcja kompresji typu ARX składa się z 12 rund 1024-bitowej permutacji P. W pojedynczej rundzie permutacji P występuje 8 łańcuchów o 4 dodawaniach modularnych. Dla 7 rund daje to 8 łańcuchów o 28 dodawaniach i na mocy lematu 6.1 prawdopodobieństwo rotacyjne przy rotacji o 1 bit równe $2^{-1015.2}$. Dla 8 rund permutacji P prawdopodobieństwo jest mniejsze od 2^{-1024}, co przeczy istnieniu rozróżniacza rotacyjnego dla 12 rund, opublikowanego w pozycji [55] spisu literatury (str. 125-127).

13. Zastosowanie lematu 6.1 do kryptoanalizy rotacyjnej funkcji skrótu Skein

Funkcja skrótu Skein zakwalifikowana została do finału konkursu na SHA-3. Funkcja kompresji typu ARX oparta jest na 72-rundowym szyfrze blokowym Threefish o bloku długości 512 bitów. W R rundach szyfru występują 4 łańcuchy o R dodawaniach modularnych. Dla 28 rund daje to 4 łańcuchy o 28 dodawaniach i na mocy lematu 6.1 prawdopodobieństwo rotacyjne przy rotacji o 1 bit równe w przybliżeniu 2^{-508}, a zatem większe od prawdopodobieństwa 2^{-512} dla losowej permutacji. W pozycji [67] spisu literatury opublikowano rozróżniacz rotacyjny dla 55 rund szyfru, ale z zastosowaniem rotacyjnych par z korekcją (str. 127-129).

14. Zastosowanie lematu 6.1 do kryptoanalizy rotacyjnej funkcji skrótu SIMD-512

Funkcja skrótu SIMD-512, analizowana w podrozdziale 5.5, zakwalifikowana została do drugiej rundy konkursu na SHA-3. Funkcja kompresji jest oparta na 36-rundowym rozszerzonym szyfrze Feistela, a stan ma długość 1024 bity (rys. 6.5). W wyniku szczegółowej analizy łańcuchów dodawań modularnych i zastosowania lematu 6.1 uzyskano dla 20 rund rozróżniacz rotacyjny o prawdopodobieństwie $2^{-569.6}$ większym od prawdopodobieństwa 2^{-1024} dla losowej permutacji (str. 129-130).

15. Opracowanie autorskich narzędzi programowych

Dla potrzeb rozprawy wykonano zestaw autorskich narzędzi programowych w celu: przeprowadzenia eksperymentu na szyfrze mCrypton (str. 51-52), wyznaczenia ścieżek ze skróconymi różnicami dla szyfru SAFER++ (str. 53-55), potwierdzenia ataków na szyfr IDEA (str. 77-78), obliczenia prawdopodobieństwa rotacyjnego łańcuchów dodawań modularnych (str. 122-123) i zapewne innych obliczeń.

Za wartościowe w rozprawie uważam również:

- opis zastosowań funkcji skrótu (str. 4-7),
- opis standardów bezpiecznych algorytmów skrótu (str. 10-12),
- opis architektur funkcji skrótu i metod konstrukcji funkcji kompresji (str. 17-22),
- zestawienie jednoblokowych i dwublokowych trybów pracy szyfrów blokowych w funkcjach skrótu (str. 23-24),
- przedstawienie ataku odbiciowego, typu „rebound", na szyfr SP (str. 30-32),
- opis kryptoanalizy rotacyjnej (str. 34-38),
- analizę złożoności ataków na szyfry Feistela w modelach ze znanym kluczem i z wybranym kluczem (str. 55-57),
- analizę prowadzącą do wniosku, że atak kolizyjny na funkcję skrótu z szyfrem IDEA w trybie Davies-Meyer ma złożoność $2^{16.13}$ (str. 68-71).

Pytania szczegółowe dotyczące rozprawy:

1. W jakim stopniu niniejsza rozprawa różni się od rozprawy Autora [115], zatytułowanej „Contributions to Cryptanalysis: Design and Analysis of Cryptographic Hash Functions"?

2. W jakim stopniu treść rozdziałów 3, 4, 5 i 6 niniejszej rozprawy różni się od odpowiadających im publikacji z udziałem Autora [109], [125], [110] i [65]?

3. Jakie narzędzia programowe wykorzystane zostały do przeprowadzenia badań przedstawionych w niniejszej rozprawie?

4. Jak przebiega analiza złożoności ataków różnicowych na szyfr DES w modelach ze znanym kluczem i z wybranym kluczem?

4. Ocena redakcji rozprawy

Rozprawa pod względem redakcji posiada wiele pozytywnych, godnych podkreślenia cech. Jest napisana bardzo dobrym językiem. Ma wyodrębnione, numerowane podrozdziały, a w wielu z nich wyodrębnione, numerowane punkty – jest strukturalnie zorganizowana. Tekst podzielony jest na logicznie wyodrębnione akapity – jest czytelny. W wielu miejscach stosowane są wypunktowania. Rozprawa jest także bogato ilustrowana – zawiera 21 rysunków i 18 tabel. Na wyróżnienie zasługują rysunki 3.1, 3.2 i 3.3 (str. 50-51) ilustrujące ścieżki o skróconych różnicach, rysunki 3.5 i 3.6 (str. 54-55) ilustrujące ścieżki o standardowych różnicach oraz rysunki 6.3 (str. 126), 6.4 (str. 128) i 6.5 (str. 131) ilustrujące łańcuchy dodawań modularnych w funkcji kompresji. Główne formuły są wyodrębnione i selektywnie numerowane. Rozdziały od 3 do 6 zawierają podsumowanie wyników. Rozprawa ma bogatą bibliografię (127 pozycji) i liczne do niej odwołania w tekście.

Za uchybienia redakcyjne w rozprawie uważam:

1. Obecność tzw. wiszących tekstów (tj. bez numeracji, na początku rozdziału z numerowanymi podrozdziałami). Wiszące teksty w rozdziałach stosowane są konsekwentnie, ale mają niejednolitą strukturę. Np. wiszący tekst w rozdziale 1 ma charakter merytoryczny, w rozdziale 2 opisuje organizację rozdziału, w rozdziale 3 składa się z omówienia i organizacji, a w rozdziale 4 składa się z części merytorycznej, opisowej i organizacyjnej. Wiszące teksty występują też w podrozdziałach. Szczególnie kontrowersyjny jest w podrozdziale 5.4 (str. 100) o jedynym, nie wiadomo dlaczego, punkcie 5.4.1. Wiszące teksty powinny być zastąpione numerowanym wprowadzeniem, podobnie jak podsumowania, lub być pominięte.
2. Obecność powtórzeń zagadnień w rozdziałach 1 i 2. Własności kryptograficznej funkcji skrótu w podrozdziale 1.1 (str. 1) są powtórzone z zastosowaniem innych oznaczeń w definicji 2.2 (str. 16). Metody kryptoanalizy niezależne od algorytmu w punkcie 1.4.1 (str. 7-8) są powtórzone, z pominięciem jednej, w punkcie 2.5.1 (str. 25-27). Metody kryptoanalizy zależne od algorytmu w punkcie 1.4.2 (str. 8-10) są powtórzone, z pominięciem trzech, w punktach 2.5.2 (str. 27) i 2.5.3 (str. 34) oraz dodaniem jednej w punkcie 2.5.4 (str. 38). Ponadto zawartość punktu 2.5.5, tj. definicje T-funkcji i S-funkcji, zupełnie nie mieści się w rozdziale 2.5 (str. 25) poświęconemu metodom analizy. W rozdziale 1 omawiane są również zagadnienia nie rozwinięte w rozdziale 2. Zawartość rozdziałów 1 i 2 nie została starannie przemyślana.

3. Obecność złej organizacji podrozdziału 5.4. Tytuł podrozdziału nie odpowiada jego zawartości. W punkcie 5.4.1 powinien być przedstawiony algorytm ulepszonego ataku, w punkcie 5.4.2 ulepszony atak na BMWv1, a w punkcie 5.4.3 ulepszony atak na zmodyfikowaną wersję BMWv2, oznaczoną jako $BMWv2_C$. Inne oznaczenia wariantów funkcji skrótu BMW-512 poza wymienionymi trzema nie powinny być używane. Zatem stosowane oznaczenia, takie jak BMW, BMWv1-512, BMWv2-512, należy uznać za niewłaściwe.
4. Brak konsekwencji w kolejności. Na stronie 41 przy omawianiu zawartości rozdziału 3 omawiane są podrozdziały w kolejności 3.1, 3.3 i 3.2. W tabeli 3.2 (str. 44) i tabeli 4.6 (str. 77) kolejność trybów dwublokowych jest inna niż w tabeli 2.2 (str. 24). W tabeli 3.3 (str. 58) i na początku podrozdziału 3.3 (str. 48) kolejność szyfrów nie odpowiada kolejności ich analizy w punktach 3.3.1 (str. 49) i 3.3.2 (str. 53). W tabeli 5.6 (str. 113) kolejność funkcji skrótu nie odpowiada kolejności ich analizy w podrozdziałach 5.5 (str. 103) i 5.6 (str. 109). Kolejność lematów 5.4, 5.5, i 5.6 (str. 110) jest niewłaściwa co skutkuje chaosem w dowodach tych lematów (str. 111-112).
5. Obecność drobnych błędów, w tym językowych. Np. na stronie 15 występuje oznaczenie $\{0, 1\}^*$ dla zbioru niepustych ciągów zerojedynkowych zamiast bardziej właściwego oznaczenia $\{0, 1\}^+$, w definicji 2.4 (str. 18) występuje błąd zarówno przy indeksowaniu bloków wiadomości od 0 jak i od 1, na rysunku 2.1 (str. 19) występuje inne indeksowanie niż w definicji 2.4 (str. 18), na stronie 19 w formule zapisanej w ostatniej linii występują 3 błędy, na stronie 20 występuje „paralellization" zamiast „parallelization", na stronie 21 dwukrotnie występuje zmienna r zamiast zmiennej k, na stronie 23 występuje „(paragraph split)", na stronie 24 występuje „MHJ" zamiast „MJH", na stronie 30 dwukrotnie występuje „differences" zamiast „difference" i „Δ'_i" zamiast „Δ'_1", na stronie 34 występuje „2^{16}" zamiast „2^b", na stronie 36 występuje „p_F" zamiast „$p_F < 1$", na stronie 44 nie jest objaśniony tryb MDC-2 występujący w tabeli 3.2, na stronie 45 występuje niejasne odwołanie do punktu 2.5.2, na stronie 48 występuje „to be higher" zamiast „are higher", na stronie 50 występuje odwołanie do punktu 2.5.2 gdzie wpływ długości klucza nie jest wyjaśniony, na stronie 66 pojawiają się zmienne CV i M w miejsce dotąd stosowanych h i m, na stronie 81 występuje „2.5.3" zamiast „section 2.5.3", na stronie 109 permutacja P oznaczana jest jako $P_{M,C}(A, B)$, a na stronie 112 jako $P(A, B, C, M)$, na stronie 113 w nagłówku tabeli 5.6 brakuje funkcji „SIMD", na stronie 119 występuje „6.1" i „6.5" zamiast „(6.1)" i „(6.5)", na stronie 126 występują zmienne m_i i m_j zamiast m_1 i m_2.

5. Wniosek końcowy

Recenzowana rozprawa składa się z dwóch głównych części. Część pierwsza, obejmująca rozdziały 1 i 2, ma charakter wstępny. Opisano w niej kryptograficzne funkcje skrótu, a w szczególności metody projektowania i analizy tych funkcji. W części drugiej, obejmującej rozdziały 3, 4, 5 i 6, przedstawiono wyniki Autora w zakresie analizy kryptograficznych funkcji skrótu.

Pierwsza grupa wyników dotyczy kryptograficznych funkcji skrótu zbudowanych w oparciu o szyfr blokowy. W tym zakresie określono najlepsze różnicowe ataki kolizyjne na tryby pracy szyfru blokowego w funkcji kompresji, przedstawiono dowód lematu o dolnej granicy złożoności różnicowego rozróżniacza dla losowej permutacji, wyznaczono różnicowe rozróżniacze dla szyfrów Crypton, Hierocrypt-3 i Square w modelach ze znanym kluczem i z wybranym kluczem, skonstruowano atak odbiciowy, typu „rebound", na 6.5-rundowy SAFER++ z kluczem 128-bitowym w modelu z wybranym kluczem oraz skonstruowano ataki kolizyjne i preobrazowe na tryby pracy szyfru IDEA w funkcji kompresji.

Druga grupa wyników dotyczy kryptograficznych funkcji skrótu zbudowanych jako konstrukcje typu ARX. W tym zakresie rozszerzono kryptoanalizę rotacyjną na elementarne operacje spoza zestawu operacji ARX (dodawanie arytmetyczne, rotacja, operacja XOR), przedstawiono rozszerzenie kryptoanalizy rotacyjnej na rotacyjne pary z korekcją oraz sposób obliczania prawdopodobieństwa tych par dla operacji dodawania, wyznaczono rotacyjne rozróżniacze dla funkcji skrótu BMW-512 i SIMD-512, wprowadzono kryptoanalizę przesunięciową i wyznaczono przesunięciowe rozróżniacze dla funkcji skrótu Shabal, sformułowano i udowodniono lemat o prawdopodobieństwie rotacyjnym łańcuchów dodawań modularnych oraz zastosowano ten lemat do kryptoanalizy rotacyjnej funkcji skrótu BLAKE2, Skein i SIMD-512.

Redakcja rozprawy jest staranna, a jej układ jest przejrzysty. Występują nieliczne błędy i usterki redakcyjne. Sformułowane zarzuty odnośnie redakcji mają znaczenie drugorzędne. Przygotowanie rozprawy w przedstawionej formie wymagało ogromnej pracy.

Podsumowując należy podkreślić, że rozprawa zawiera bardzo wiele ważnych i oryginalnych wyników, a także świadczy o głębokiej wiedzy Autora odnośnie kryptoanalizy szyfrów blokowych i kryptograficznych funkcji skrótu.

Stwierdzam, że recenzowana rozprawa doktorska pana magistra Przemysława Sokołowskiego zatytułowana „Design and Analysis of Cryptographic Hash Functions" spełnia wymagania *Ustawy o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki* bez zmian wprowadzonych *Ustawą z dnia 18 marca 2011 r. o zmianie ustawy – Prawo o szkolnictwie wyższym, ustawy o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki oraz o zmianie niektórych innych ustaw* (Dz. U. Nr 84 poz. 455) oraz uzasadnia nadanie panu magistrowi Przemysławowi Sokołowskiemu stopnia naukowego doktora nauk matematycznych w zakresie informatyki.

Krzysztof Chmiel

.....

Krzysztof Chmiel