dr hab. inż. Janusz Stokłosa
prof. w Wyższej Szkole Bankowej w Poznaniu

Poznań, 24 lipca 2019 r.

Recenzja rozprawy doktorskiej mgr. inż. Marcina Dawca

pt. „**Problem wyszukiwania kostek w kontekście kryptoanalizy szyfrów blokowych**"

wykonana dla

Rady Wydziału Cybernetyki Wojskowej Akademii Technicznej w Warszawie

1. Przedłożona mi do recenzji rozprawa doktorska mgr. inż. Marcina Dawca dotyczy kryptoanalizy symetrycznych algorytmów kryptograficznych, w szczególności szyfrów blokowych. Przedstawiono w niej atak polegający na wykorzystaniu pewnych podatności funkcji boolowskich występujących w konstrukcjach algorytmu kryptograficznego, zwany atakiem za pomocą kostek.

Głównym celem pracy było pokazanie, że istnieją inne niż znane dotąd z literatury sposoby poszukiwania kostek, które są realizowalne praktycznie w tym sensie, że istnieje możliwość ich zaimplementowania na komputerach roboczych lub niewielkich klastrach obliczeniowych.

2. Rozprawa składa się z siedmiu rozdziałów, wykazu literatury, dwóch załączników, spisu rysunków, tabel i algorytmów, listy najważniejszych symboli, a także streszczeń w języku polskim i angielskim – razem 104 strony.

Rozdziałem 1 jest wstęp do rozprawy, w którym Autor zarysował problematykę badawczą, określił cel i zakres pracy badawczej oraz przedstawił układ pracy.

Rozdział 2 jest zwięzłym wprowadzeniem do kryptologii. Autor zdefiniował szyfr blokowy, poświęcił uwagę trybom pracy tych szyfrów omawiając szczegółowiej trzy tryby: ECB, CBC oraz CTR. W podrozdziale poświęconym kryptoanalizie przedstawił modele ataków oraz zwrócił uwagę na zasadę Kerckhoffsa. Sporo miejsca poświęcił funkcjom boolowskim i ich roli w kryptografii. Skoncentrował się na dwóch operacjach wykonywanych na funkcjach boolowskich: dodawaniu i mnożeniu. W ramach badań nad skutecznym poszukiwaniem kostek Autor porównał eksperymentalnie kilka algorytmów mnożenia funkcji boolowskich.

Metody kryptoanalizy korzystające z kostek są przedmiotem rozważań zawartych w rozdziale 3. Pierwszy atak za pomocą kostek wykonali Adi Shamir oraz Itai Dinur w 2009 roku.

Autor przedstawia ideę tego ataku, w którym wykorzystano fakt, że funkcje boolowskie opisujące bity szyfrogramu zależą od bitów tajnego klucza oraz bitów wiadomości jawnej. Kryptoanalityk może zmieniać algebraiczną postać normalną (APN) funkcji poprzez przypisanie wybranych wartości zmiennym jawnym i wykonanie tzw. sumowania po kostce. Algebraicznej postaci normalnej funkcji boolowskiej odpowiada wielomian wielu zmiennych. Przypisując zmiennym jawnym w takim wielomianie wszystkie możliwe wartości ze zbioru {0, 1} uzyskuje się wielomiany pochodne i w wyniku sumowania niektórych z nich można uzyskać dający się rozwiązać układ równań. Celem kryptoanalityka jest rozwiązanie wynikowego układu równań, w którym niewiadomymi są wyłącznie zmienne tajne. W rozdziale 3 Autor opisuje przede wszystkim w sposób formalny tę metodę ataku. Punktem wyjścia jest tu pojęcie kostki. Dowolny podzbiór indeksów I o liczności k definiuje k-wymiarową kostkę boolowską C_I zawierającą 2^k wektorów, w których zmiennym o indeksach ze zbioru I przypisywane są wszystkie możliwe wartości, a wartości pozostałych zmiennych (jawnych i tajnych) są nieokreślone. Każdy wektor kostki C_I określa wielomian pochodny, a suma wielomianów pochodnych dla wszystkich 2^k wektorów z kostki C_I tworzy nowy wielomian p_I, odpowiadający tzw. superwielomianowi $p_{S(I)}$ (przystający do niego modulo 2). To udowodnione przez Shamira i Dinura twierdzenie, jest niezwykle przydatne w kryptoanalizie.

Poszukiwanie superwielomianów liniowych jest procesem charakteryzującym się zwykle dużą złożonością obliczeniową i stanowi fazę wstępną ataku. Druga faza ataku, w której kryptoanalityk dąży do wyznaczenia zastosowanego klucza nazywana jest fazą *online*. Autor opisuje dokładnie obydwie fazy ataku. Poświęca także uwagę: (i) testom wykonywanym za pomocą kostek, których celem jest odróżnianie wyjścia algorytmu kryptograficznego od wyjścia funkcji losowej, czyli wykrywania braku losowości, poprzez badanie własności algebraicznych superwielomianów; (ii) atakom za pomocą kostek dynamicznych; (iii) atakom podobnym do kostkowych (*cube-like*), (iv) atakom za pomocą kostek warunkowych.

W rozdziale 4 Autor przedstawił metody poszukiwania kostek. Omówił (i) metodę losową, (ii) metodę polegającą na analizie struktury szyfru, (iii) metodę wykorzystującą mieszane programowanie całkowitoliczbowe, (iv) przeszukiwanie algebraicznej postaci normalnej wielomianów głównych – pomysł autorski, rozwinięty do opracowania techniki konstrukcji zredukowanej algebraicznej postaci normalnej wielomianów głównych i ich przeszukiwania (mianem wielomianów głównych określane są funkcje boolowskie bitów wyjścia algorytmu; w przypadku szyfrów blokowych są to funkcje boolowskie, w których zmiennymi są bity tekstu jawnego i bity klucza, a wartościami bity szyfrogramu). Autor zdefiniował kostkę liniową (w kontekście algebraicznej postaci normalnej) w wielomianie jako taki iloczyn zmiennych jawnych, że po wyłączeniu go przed nawias, w nawiasie pozostaje suma jednomianów stopnia 1, zawierających tylko zmienne klucza.

Autor pokazał sposób poszukiwania kostek w sytuacji, gdy atakujący zna konstrukcję algorytmu i ma możliwość rekurencyjnego wyznaczania wielomianów głównych. W rezultacie zmniejszeniu ulega zbiór kostek, a poprawie skuteczność ich znajdowania.

Rozdział 5 dotyczy poszukiwania kostek w szyfrach blokowych. Autor skoncentrował się na dwóch metodach poszukiwania kostek dla szyfrów blokowych: losowej i wynikającej z analizy zredukowanych APN wielomianów głównych. Pierwsza ma tę zaletę, że można ją zastosować do algorytmów o nieznanej konstrukcji. W przypadku drugim Autor rozważa iteracyjne szyfry blokowe, których konstrukcja zasadza się na wielokrotnym wykonywaniu przekształcenia rundowego.

Rozdział 6 Autor poświęcił kryptoanalizie szyfrów blokowych zwracając uwagę na implementacyjne aspekty ataku za pomocą kostek, a w drugiej przedstawił atak na szyfr CTC (ang. *Courtois Toy Cipher*). Wyznaczanie klucza szyfru za pomocą znajomości superwielomianów jest celem realizacji fazy *online* ataku za pomocą kostek. Atak wymaga dostępu do urządzenia szyfrującego i dysponowania układem równań superwielomianów oraz skojarzonych z każdym superwielomianem zbiorem indeksów i numerem wielomianu głównego. Autor opracował narzędzie działające jednowątkowo, umożliwiające (i) wczytanie układu superwielomianów, (ii) obliczenie wartości wyrazu wolnego każdego superwielomianu poprzez wykonanie sumowania po kostce, (iii) rozwiązanie układu superwielomianów.

Do poszukiwania kostek i przeprowadzenia ataku na szyfr CTC ograniczony do 4 i 5 rund, w którym blok danych i długość klucza wynoszą 120 bitów Autor zastosował opracowaną przez siebie metodę analizy zredukowanych APN wielomianów głównych. Znalazł zbiory indeksów definiujące kostki. Zbadał skuteczność sposobów poszukiwania kostek dla 4-rundowego szyfru dla metody losowej znajdowania zbiorów indeksów o liczności 4 oraz metody opartej na analizie APN o liczbie zmiennych publicznych ograniczonej do 16, 8 i 6. Wykazał, że dla atakowanego szyfru 4-rundowego najbardziej skuteczna jest metoda losowa oraz działająca na wielomianach 6 zmiennych, lecz ograniczona do zbiorów indeksów o liczności 4. W przypadku szyfru 5-rundowego zbiory indeksów definiujących superwielomiany liniowe znaleziono wyłącznie korzystając z metody polegającej na analizie wielomianów głównych w zredukowanej postaci APN.

W rozdziale 7 podsumowano uzyskane w rozprawie wyniki oraz wskazano kierunki dalszych badań.

3. Rozprawa ma charakter teoretyczno-eksperymentalny. Autor trafnie wybrał obszar badań. Głównym osiągnięciem Autora rozprawy jest opracowanie metody poszukiwania kostek za pomocą analizy zredukowanej algebraicznej postaci normalnej wielomianów głównych. Ma ona dwie istotne właściwości: (i) można ją stosować w różnych środowiskach obliczeniowych, (ii) zwraca zbiór zawierający wszystkie kostki. Opracowaną przez siebie metodę poszukiwania kostek Autor zastosował z sukcesem do ataku na ograniczoną do pięciu rund wersję 120-bitowego szyfru blokowego CTC. Do tej pory najskuteczniejszym atakiem na ten szyfr wykorzystującym kostki był atak na jego wersję 4-rundową. Autor słusznie zwraca uwagę na ograniczenia zaproponowanej przez siebie metody ataku na szyfry blokowe: (i) dużą złożoność pamięciową, (ii) konieczność mnożenia funkcji boolowskich, (iii) skuteczność wyłącznie dla kilku początkowych rund. Aby usprawnić mnożenie funkcji boolowskich Autor zaproponował opracowane przez siebie dwie metody możliwe do stosowania w urządzeniach wyposażonych w niedużą pamięć operacyjną.

Autor słusznie zwraca uwagę na to, że ocena bezpieczeństwa dowolnego algorytmu kryptograficznego powinna być kompletna, tzn. powinien on być odporny na wszystkie znane metody ataków, w tym także na ataki wykorzystujące kostki. Z tego powodu osiągnięcie mgr. inż. Marcina Dawca należy uznać za pewien krok zmierzający do tego celu.

Praca napisana jest językiem zrozumiałym i zwięzłym. Usterek spostrzegłem niewiele, nie wpływają one na zrozumienie wywodu. Mam jednak następujące uwagi krytyczne:

(i) spis treści jest niekompletny,

(ii) definicja usługi weryfikacji integralności danych (str. 15) jest niepoprawna; także w sposób niejasny Autor sugeruje wykorzystywanie funkcji skrótu i kodów uwierzytelniających wiadomość do uwierzytelniania danych,

(iii) opisując usługę niezaprzeczalności (str. 15) Autor wskazuje, że może ona „być realizowana poprzez wykorzystanie algorytmów podpisu cyfrowego"; czy tylko?,

(iv) na rysunkach 2.3 – 2.7 wiadomość jawna jest oznaczana błędnie symbolem P zamiast M,

(v) na str. 44 i następnych wprowadzono operację + nie wyjaśniając jej znaczenia; podobnie na str. 64 w odniesieniu do operacji $\odot$,

(vi) na str. 50 stwierdzenie, że „Tablica prawdy takiej funkcji boolowskiej będzie przypominać ciąg losowy" jest dyskusyjne,

(vii) na str. 94 niezrozumiałe jest pojęcie funkcji „opartych na 13 zmiennych",

(viii) poza jednym przypadkiem (twierdzenie 2.23, str. 28) brak jest informacji o źródłach prezentowanych w rozprawie twierdzeń.

4. Reasumując stwierdzam, że:
   - teza rozprawy została wykazana,
   - rozprawa stanowi oryginalne rozwiązanie problemu naukowego,
   - tematyka rozprawa jest aktualna i ważna,
   - Autor rozwiązał zdefiniowany przez siebie problem naukowy i użył do tego celu odpowiednich metod, tak więc wykazał się umiejętnością samodzielnego prowadzenia badań naukowych,
   - rozprawa świadczy o dużej wiedzy teoretycznej mgr. inż. Marcina Dawca w zakresie kryptoanalizy szyfrów blokowych.

Przedstawiona mi do recenzji dysertacja doktorska, mieszcząca się w dyscyplinie naukowej informatyka, spełnia wymagania stawiane rozprawom doktorskim w *Ustawie o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki* z dnia 14 marca 2003 r. (Dz. U. nr 65, poz. 595; tekst ujednolicony Dz.U. z 2017 r. poz. 1789).

Wnoszę o dopuszczenie mgr. inż. Marcina Dawca do publicznej obrony rozprawy.