Warszawa, 28 października 2019r.

**dr hab. Mirosław Kurkowski**
**prof. nzw. UKSW, prof. nzw. WSPol**
- **Instytut Informatyki**

**Uniwersytet kard. St. Wyszyńskiego w Warszawie**
- **Zakład Cyberbezpieczeństwa**

**Wyższa Szkoła Policji w Szczytnie**

# Recenzja rozprawy doktorskiej mgra Ashutosha Dhar Dwivedi

## *Cryptanalysis of lightweight ciphers*

## Promotor: prof. IPI PAN, dr hab. Paweł Morawiecki

Recenzja niniejsza została sporządzona na prośbę Rady Naukowej Instytutu Podstaw Informatyki PAN w Warszawie. Opiniowana rozprawa napisana jest w języku angielskim. Dotyczy ona analizy wybranych szyfrów tzw. kryptografii lekkiej, czyli algorytmów działających w środowiskach o mocno ograniczonych zasobach obliczeniowych i pamięciowych. Przewód doktorski prowadzony jest w dziedzinie nauk technicznych, w dyscyplinie naukowej Informatyka.

### Wprowadzenie

Kryptografia jest wciąż prężnie rozwijającą się dyscypliną nauki. Jej znaczenie w dobie społeczeństwa informacyjnego jest ogromne. Nikt nie wyobraża sobie systemów komunikacji i wymiany danych bez odpowiednich zabezpieczeń. Wciąż rozwijające się technologie oraz stale postępująca miniaturyzacja i powszechność urządzeń służących do komunikowania się stawiają nowe wyzwania również dla algorytmów kryptograficznych. Często mamy do czynienia z koniecznością zabezpieczania urządzeń lub łącz komunikacyjnych mając do dyspozycji bardzo małe zasoby obliczeniowe lub/oraz pamięciowe. Dobrymi przykładami są coraz mniejsze urządzenia mobilne. Nie ma zatem wątpliwości, że tematyka badawcza poruszana w rozprawie mgra Ashutosha Dwivedi jest aktualna i ważna dla dzisiejszej szeroko pojętej informatyki.

### Zawartość rozprawy

Recenzowana rozprawa składa się z Wprowadzenia, pięciu rozdziałów, Podsumowania oraz Bibliografii. Ogólny układ rozprawy moim zdaniem nie budzi zastrzeżeń. Bibliografia zawiera 80 pozycji i w mojej opinii dobrana została właściwie.

We Wprowadzeniu oprócz ogólnego zarysu prowadzonych badań i ich tła autor przedstawia cele rozprawy i hipotezy badawcze. Głównym celem pracy „…*jest ocena marginesu bezpieczeństwa wybranych szyfrów kryptografii lekkiej czyli algorytmów działających w środowiskach o mocno ograniczonych zasobach obliczeniowych i pamięciowych*.” Do realizacji założonego celu wybrano współczesne metody i techniki kryptoanalityczne wzbogacone o autorskie udoskonalenia.

Doktorant określił trzy hipotezy badawcze, które poddał weryfikacji w toku swoich badań:

1) Szyfr SCREAM ma niedostateczny margines bezpieczeństwa dla wariantu dedykowanego lekkiej kryptografii.

2) Heurystyki używane w grach z jednym graczem (np. Sudoku) mogą być z powodzeniem zastosowane i ulepszone do poszukiwania ścieżek różnicowych w algorytmach klasy ARX (Addition, Rotation, XOR).

3) Kryptoanaliza SAT (kryptoanaliza logiczna) pozwala na szybkie, praktyczne ataki na pewne redukcje szyfru ASCON.

Treść i znaczenie powyższych hipotez już na początku czytania pracy stawia badane problemy wysoko i w pełni uzasadnia prowadzone badania.

Na koniec Wprowadzenia autor dokonuje przeglądu literatury i omawia pokrótce najnowsze osiągnięcia w rozważanym zakresie.

Pierwszy rozdział zawiera wprowadzenie do kryptografii ze szczególnym uwzględnieniem technik kryptoanalitycznych. Autor przedstawia główne architektury stosowane obecnie w kryptografii symetrycznej (Feistel, SPN, ARX), opisując dokładnie ich zalety i wady. W Podrozdziale 1.5 znajdują się podstawowe definicje i pojęcia związane z kryptoanalizą oraz krótki przegląd scenariuszy i modeli ataku.

Moim zdaniem wstępne części rozprawy wprowadzające podstawowe pojęcia i struktury potrzebne do dalszych rozważań 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.

W rozdziale drugim zaprezentowane są najważniejsze techniki kryptoanalityczne, które były użyte w pracy i stanowiły podstawę do autorskich, nowych rozwiązań. Opisana została kryptoanaliza liniowa, różnicowa i wariant kryptoanalizy różnicowej (ang. impossible differential cryptanalysis). Dodatkowo doktorant przybliża na czym polega atak w scenariuszu z kluczem powiązanym (ang. related-key attack).

Rozdział trzeci w całości poświecony jest szyfrowi SCREAM. Szyfr SCREAM jest interesującą konstrukcją, w której mamy dodatkowy parametr nazwany tweak, który pełni podobną rolę jak wektor inicjalizujący w szyfrach strumieniowych. Do kryptoanalizy tego szyfru użyte zostały dość standardowe techniki kryptoanalizy liniowej i różnicowej.

Kolejny, najdłuższy rozdział to kryptoanaliza różnicowa dla szyfrów z klasy ARX, ze szczególnym uwzględnieniem algorytmów SPECK i LEA. Szyfr SPECK został zaprojektowany przez Amerykańską Agencję Bezpieczeństwa (ang. National Security Agency) i jest bardzo dobrym rozwiązaniem dla środowisk o ograniczonych możliwościach pamięciowo-obliczeniowych. Szyfr LEA, podobnie jak SPECK, bazuje na trzech operacjach: dodawanie modulo, rotacja i bitowy XOR. Doktorant prezentuje heurystykę do szukania ścieżek różnicowych dla szyfrów ARX, gdzie tradycyjne metody (stosowane w algorytmach typu AES) zawodzą.

Rozdział piąty dotyczy kryptoanalizy szyfru ASCON - jednego ze zwycięzców konkursu CAESAR. Zastosowana metoda to kryptoanaliza logiczna polegająca na opisaniu szyfru (lub jego fragmentu) formułą, którą dalej rozwiązuje tester SAT (ang. SAT-solver).

Praca zawiera krótkie Podsumowanie, gdzie uzyskane wyniki przedstawione są w kontekście hipotez badawczych nakreślonych we Wstępie.

**Opinia merytoryczna rozprawy**

Za najważniejszy wynik uważam algorytm do szukania ścieżek różnicowych dla algorytmów klasy ARX opisany w rozdziale czwartym. Autor zaczerpnął inspirację ze stosunkowo prostej (lecz efektywnej) metody przeszukiwania drzew w grach jednoosobowych takich jak Sudoku czy pewne warianty gier karcianych. Wyszukiwanie dobrych ścieżek różnicowych (ang. differential path) również można potraktować jako grę — stąd też inspiracja.

Warto podkreślić, że wyniki z rozdziału czwartego zostały opublikowane w czasopiśmie IEEE Access (lista A, obecnie 100 pkt. na nowej liście czasopism), w artykule „*Differential Cryptanalysis of Round-Reduced SPECK Suitable for Internet of Things*". Doktorant zaaplikował opracowaną metodę również do innych szyfrów lekkiej kryptografii co zaowocowało publikacją „*Cryptanalysis of Round-Reduced Fantomas, Robin and iSCREAM*" w czasopiśmie Cryptography.

Wyniki kryptoanalizy różnicowo-liniowej dla szyfru SCREAM zostały opublikowane w czasopiśmie Information Processing Letters w artykule „*Differential-linear and related key cryptanalysis of round-reduced Scream*" w 2018 r. Wcześniej natomiast cząstkowe wyniki były prezentowane na konferencji SECRYPT w 2017 r.

Również analiza z użyciem testerów SAT (wyniki z Rozdziału 5) zostały zaprezentowane na konferencji SECRYPT w artykule „*SAT-based Cryptanalysis of Authenticated Ciphers from the CAESAR Competition*”.

Wymienione publikacje mają łącznie 24 cytowania (bez autocytowań), dane za Google Scholar. Świadczy to o dobrej rozpoznawalności, szczególnie, że czas od publikacji nie przekracza 2.5 roku.

**Uwagi polemiczne i krytyczne**

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

Do analizy szyfru SCREAM (Rozdział trzeci) zostały wykorzystane standardowe techniki takie jak kryptoanaliza różnicowa i liniowa oraz wariant różnicowej tzw. różnice niemożliwe (ang. impossible differential cryptanalysis). Pewne rozczarowanie budzi fakt, że mało jest tutaj próby wprowadzenia nowego pomysłu, wzbogacenia tych klasycznych technik. Sytuację trochę ratuje użycie dodatkowego parametru (tweak) w scenariuszu, gdzie atakujący ma nad nim kontrolę i dzięki temu konstruuje dłuższe charakterystyki różnicowe.

Podobną uwagę można odnieść na kryptoanalizy SAT dla szyfru ASCON. Autor postępuję wg utartej ścieżki (konstrukcja formuły boolowskiej, konwersja do CNF i próba rozwiązania testerem SAT). To co stanowi oryginalny wkład własny w tym fragmencie pracy to przemyślany wybór, który fragment algorytmu poddać temu atakowi i w jakim scenariuszu. Zakodowanie całego szyfru w postaci CNF i próba rozwiązania przez SAT jest zadaniem o zbyt dużej złożoności w rozsądnym czasie. Jednakże można było się pokusić o bardziej wnikliwą analizę np. rozpatrując różne sposoby budowania formuł i obserwując jak się to przekłada na czas ataku. Uważam również, że wyniki tego rozdziału zasługują na bardziej szczegółowy opis.

**Uwagi redakcyjne**

Jak każda praca naukowa również recenzowana rozprawa nie jest wolna od niedociągnięć, pomyłek, czy błędów natury redakcyjnej. Zdarzają się zwykłe literówki jak na przykład: *cryptograhy, cryptogrpahy, extensisve, roundreduced, characteristc*. Czasem pewne wątpliwości budzą zapisy matematyczne. Trzeba jednak stwierdzić, że rozprawa mgra Ashutosha Dhar Dwivedi została przygotowana bardzo staranie i zawiera wyjątkowo mało takich błędów. Należy podkreślić pozytywnie jakość i adekwatność schematów oraz rysunków, które w znakomity sposób obrazują prowadzone rozważania. Może należałoby również lepiej opracować technicznie Bibliografię – poszczególne pozycje są przedstawiane w różnych stylach.

**Wniosek końcowy**

Przedstawione w recenzowanej rozprawie doktorskiej rozważania związane z analizą wybranych szyfrów tzw. kryptografii lekkiej, czyli algorytmów działających w środowiskach o mocno ograniczonych zasobach obliczeniowych i pamięciowych dotyczą bieżących, ważnych i interesujących problemów naukowych związanych z konstrukcją i metodami analizy współczesnych systemów kryptograficznych. Rozprawa doktorska mgra Ashutosha Dhar Dwivedi 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 Ashutosha Dhar Dwivedi 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 Ashutosha Dhar Dwivedi do dalszych etapów przewodu doktorskiego celem nadania Mu przez Radę Naukową Instytutu Podstaw Informatyki PAN stopnia naukowego doktora nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja.**