Autoreferat

1. **Imię i nazwisko:** Paweł Morawiecki

2. **Posiadane dyplomy**

- doktor nauk technicznych w zakresie telekomunikacji, Politechnika Warszawska 2010, Rozprawa: „Dekompozycja funkcjonalna zespołów funkcji boolowskich”
- magister inżynier, Politechnika Warszawska 2004, Wydział Elektroniki i Technik Informacyjnych
- licencjat z zarządzania, Wyższa Szkoła Handlowa w Kielcach, 2003

3. **Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych**

- 2016 - aktualnie: Instytut Podstaw Informatyki PAN (adiunkt, kierownik Zespołu Kryptografii w Zakładzie Teoretycznych Podstaw Informatyki)
- 2012-2016: Instytut Podstaw Informatyki PAN
- 2005 - 2016: Wyższa Szkoła Handlowa w Kielcach, Zakład Informatyki

4. **Wskazanie osiągnięcia wynikającego z art. 16 ust. 2 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki (Dz. U. 2016 r. poz. 882 ze zm. w Dz. U. z 2016 r. poz. 1311.):**

Jako osiągnięcie naukowe wskazuję cykl 10 monotematycznych publikacji.

4a Tytuł osiągnięcia naukowego: „Kryptoanaliza algorytmów kryptografii symetrycznej”

4b Cykl publikacji:

[1] P. Morawiecki, M. Srebrny „A SAT-based preimage analysis of reduced Keccak hash functions”, Information Processing Letters, volume 113(10-11), 2013

[2] E.Homsirikamol, P. Morawiecki, M. Rogawski, M. Srebrny „Security Margin Evaluation of SHA-3 Contest Finalists through SAT-Based Attacks”, LNCS, Proceedings of International Conference CISIM, 2012, Venice, Italy

[3] P. Morawiecki, J. Pieprzyk, M. Srebrny „Rotational Cryptanalysis of Round-Reduced Keccak", Proceedings of Fast Software Encryption (FSE), Singapore 2013, Revised Selected Papers

[4] P. Morawiecki „Malicious SHA-3", 17th Central European Conference on Cryptology, Warsaw 2017 (praca zgłoszona do specjalnego wydania Fundamenta Informaticae)

[5] I. Dinur, P. Morawiecki, J. Pieprzyk, M. Srebrny, M. Straus „Cube Attacks and Cube-Attack-Like Cryptanalysis on the Round-Reduced Keccak Sponge Function ", Proceedings of EUROCRYPT 2015, Sofia, Bulgaria 2015

[6] P. Morawiecki, K. Gaj, E. Homsirikamol, K. Matusiewicz, J. Pieprzyk, M. Rogawski, M. Srebrny, M. Wójcik „ICEPOLE: High-Speed, Hardware- Oriented Authenticated Encryption", Proceedings of Cryptographic Hardware and Embedded Systems (CHES), Busan, South Korea 2014

[7] A. Dhar Dwivedi, P. Morawiecki, S. Wójtowicz „Differential and Rotational Cryptanalysis of Round-reduced MORUS", Proceedings of SECRYPT 2017, volume 4, Madrid, Spain

[8] A. Dhar Dwivedi, M. Kloucek, P. Morawiecki, Ivica Nikolic, J. Pieprzyk, S. Wójtowicz „SAT-based Cryptanalysis of Authenticated Ciphers from the CAESAR Competition", Proceedings of SECRYPT 2017, volume 4, Madrid, Spain

[9] P. Morawiecki „Practical attacks on the round-reduced PRINCE", IET Information Security, volume 11(3), pp. 146-151, 2017

[10] A. Dhar Dwivedi, P. Morawiecki, S. Wójtowicz „Finding Differential Paths in ARX Ciphers through Nested Monte-Carlo Tree Search", International Journal of Electronics and Telecommunications, volume 64, no.2, 2018

4c Omówienie celu naukowego ww. prac i osiągniętych wyników wraz z omówieniem ich ewentualnego wykorzystania

Kryptografię — dziedzinę wiedzy o bezpiecznym przetwarzaniu i przesyłaniu informacji — zwyczajowo dzieli się na kryptografię symetryczną i asymetryczną (z kluczem publicznym). Podział ten jest do pewnego stopnia umowny, ale często przydaje się do sprecyzowania i zawężenia przedmiotu badań. W algorytmach kryptografii symetrycznej strony komunikują się ze sobą używając tego samego klucza, stąd w nazwie przymiotnik „symetryczny". Algorytmy, które mogą działać zarówno z kluczem jak i bez klucza (np. większość współczesnych funkcji skrótu) zwyczajowo również przypisuje się do rodziny kryptografii symetrycznej.

Przedmiotem badań przedstawionego cyklu prac jest kryptoanaliza algorytmów kryptografii symetrycznych takich jak szyfry blokowe, funkcje skrótu i schematy szyfrowania z uwierzytelnieniem. Wspólnym celem dla tych prac było opracowanie nowych i udoskonalenie istniejących metod kryptoanalizy. Drugi cel to przekucie doświadczeń i wyników kryptoanalitycznych na nowe pomysły w projektowaniu bezpieczniejszych algorytmów.

Kryptoanaliza stanowi obecnie podstawowe narzędzie badania i mierzenia poziomu bezpieczeństwa i wiarygodności algorytmów kryptograficznych. Współczesne rozwiązania i standardy kryptograficzne są bardzo dojrzałymi konstrukcjami, czerpiącymi z doświadczeń i wyników kryptoanalitycznych ostatnich kilku dekad. W konsekwencji coraz rzadziej mamy do czynienia ze spektakularnym złamaniem całego kryptosystemu, a uwaga kryptoanalityków przesuwa się w kierunku zredukowanych wariantów danego algorytmu (np. z mniejszą liczbą rund czy mniejszym stanem) i wyznaczania marginesu bezpieczeństwa. Badania i wyniki z przedłożonego cyklu publikacji wpisują się w to podejście do współczesnej kryptoanalizy i projektowania algorytmów kryptograficznych.

Kryptoanaliza funkcji Keccak (SHA-3) i innych funkcji skrótu

Algorytm, któremu poświęciłem najwięcej uwagi w swoich badaniach to funkcja skrótu Keccak, obecnie funkcjonująca jako standard SHA-3 [Keccak]. By mieć szersze spojrzenie na osiągnięte wyniki i ich znaczenie, warto krótko przybliżyć kontekst powstania tego algorytmu. Kryptograficzna funkcja skrótu to algorytm pobierający blok danych dowolnej długości (np. plik tekstowy, dużą prezentację multimedialną czy też rozliczenie podatkowe w formie elektronicznej) i zwracający krótki ciąg bitów o ustalonej długości. Przetwarzany blok danych zwykle nazywany jest *wiadomością* natomiast wynik obliczeń to *skrót* (ang. hash, digest). Typowe długości skrótu to 256 lub 512 bitów. Kryptograficzne funkcje skrótu znajdują zastosowanie w wielu aplikacjach i protokołach związanych z bezpieczeństwem informacji. Używane są miedzy innymi do przechowywania i weryfikacji haseł komputerowych, tworzenia sum kontrolnych plików i dokumentów, certyfikatów stron internetowych, w podpisie elektronicznym. Do niedawna jedną z najpowszechniej używanych i analizowanych funkcji skrótu była SHA-1. W 2005 roku chińskie badaczki odkryły słabość w tej funkcji i pokazały, że atak na kolizję nie wymaga tylu obliczeń ile wcześniej zakładano dla SHA-1 [Wang05]. Rezultat ten odbił się szerokim echem w środowisku naukowym i był impulsem do zorganizowania konkursu na nowy standard kryptograficznej funkcji skrótu. Konkurs zorganizował amerykański NIST (National Institute of Standards and Technology) i przyciągnął uwagę czołowych naukowców związanych z kryptologią. Zgłoszono wiele interesujących i nowatorskich propozycji i po 5 latach intensywnych badań, w 2012 roku, wyłoniono zwycięzcę. Najlepszą kryptograficzną funkcją skrótu okazał się Keccak i obecnie funkcjonuje jako nowy standard kryptograficznej funkcji skrótu SHA-3.

Moje zainteresowanie algorytmem Keccak zaczęło się jeszcze w trakcie trwania konkursu kiedy „w grze" było jeszcze kilkanaście innych algorytmów. Jednakże już wtedy było jasne, że Keccak jest nowatorską propozycją z dużym potencjałem i wnikliwa kryptoanaliza będzie

kluczowa do określenia wiarygodności tej funkcji. Keccak bazuje na nowej konstrukcji (ang. sponge construction), z którą związanych jest wiele ciekawych pytań badawczych. Funkcja ta budzi również zainteresowanie od bardziej praktycznej strony takiej jak wydajne implementacje sprzętowe i programowe. Wreszcie stanowi prawdziwe wyzwanie dla kryptoanalityków co można wywnioskować z kilku lat badań i trudności w łamaniu, znajdywaniu słabości nawet w mocno zredukowanych wariantach.

Pierwszą autorską (wspólnie z Marianem Srebrnym) kryptoanalizę funkcji Keccak przedstawiłem na tematycznej konferencji SHA-3 Workshop zorganizowanej przez NIST w Santa Barbara, USA [Morawiecki10]. Wyniki te dotyczyły kryptoanalizy logicznej (kryptoanalizy SAT) dla zredukowanych wariantów funkcji. Stephen Cook w 1971 udowodnił, że problem spełnialności (ang. SATisfiability) jest problemem NP- zupełnym. W ogólnym przypadku znalezienie wartościowania spełniającego formułę zdaniową jest praktycznie niemożliwe, lecz okazuje się, że dla wielu nawet bardzo dużych formuł, potrafimy znaleźć wartościowanie przy pomocy programów zwanych testerami SAT (ang. SAT solvers). Pierwszy związek pomiędzy testerami SAT a kryptoanalizą został pokazany w pracy [Massaci99]. Ogólna idea polega na tym by tak skonstruować formułę by rozwiązanie jej (znalezienie wartościowania) oznaczało jednocześnie znalezienie tajnego klucza (w przypadku szyfrów). Dla funkcji skrótu formuła logiczna i znalezienie dla niej wartościowania oznacza zwykle znalezienie wiadomości dla zadanego skrótu (atak na przeciwobraz). Wyniki przedstawione na konferencji SHA-3 Workshop wraz z szerszą analizą zostały opublikowane w pracy [1] wchodzącej w skład przedłożonego cyklu publikacji. Warto również zaznaczyć, że techniki kryptoanalityczne opisane w tej pracy, w tym w szczególności sposób budowania formuł SAT, poprowadziły do wygrania przeze mnie kilku kategorii w konkursie kryptoanalitycznym zorganizowanym przez autorów funkcji Keccak [Contest]. W konkursie uczestniczyły wiodące grupy badawcze w tym grupa Adi Shamira z Izreala, jak również badacze z Austrii (Graz University of Technology) i Singapuru (Nanyang Technological University).

W finałowym etapie konkursu SHA-3 obok funkcji Keccak znalazły się cztery inne bardzo interesujące funkcje skrótu (Skein [Schneier], GroestI [Gauravaram], JH [Wu], Blake [Aumasson]). We współpracy z doktorantami z George Mason University (USA), podjąłem się kryptoanalizy logicznej tych funkcji, wykorzystując doświadczenia z wcześniejszej analizy funkcji Keccak. Głównym celem tej pracy było oszacowanie marginesu bezpieczeństwa dla wszystkich 5 algorytmów i analiza porównawcza. Wyniki zostały opublikowane w [2]. Na potrzeby tej pracy opracowałem metodę i zaimplementowałem program do automatycznego generowania formuł SAT. Program jako dane wejściowe pobiera specyfikację funkcji w języku VHDL lub Verilog a następnie generuje formułę CNF (Conjunctive Normal Form) w formacie, którego używają testery SAT.

Kolejna praca [3], w której podjąłem kryptoanalizę funkcji skrótu Keccak ogniskuje się wokół techniki nazywanej kryptoanalizą rotacyjną. Technika ta została formalnie wprowadzona w pracy [Khovratovich10]. Tutaj, podobnie jak w przypadku kryptoanalizy różnicowej, obserwujemy pewną relację między parą wiadomości, lecz nie jest to różnica XOR tylko rotacja (przesunięcie bitowe) jednej wiadomości wobec drugiej. Śledząc jak długo i z jakim prawdopodobieństwem w danym algorytmie taka relacja się utrzymuje, jesteśmy w stanie wywnioskować informacje użyteczne dla ataku. Moim nowatorskim pomysłem było zastosowanie rotacyjnej analizy do zbudowania ataku na przeciwobraz. Przedstawiłem kilka ataków na warianty funkcji Keccak o zredukowanej liczbie rund. Dodatkowo w pracy tej

została przedstawiona wnikliwa analiza relacji rotacyjnych na poziomie bitów, podczas gdy we wcześniejszych pracach autorzy skupiają się na całych słowach (analiza algorytmów klasy ARX). Keccak jako algorytm zorientowany bitowo wymagał wprowadzenia nowego podejścia i zdefiniowania nowych pojęć potrzebnych do precyzyjnego opisu przeprowadzonej kryptoanalizy. Praca została zaprezentowana na konferencji Fast Software Encryption (FSE) w 2013 roku w Singapurze. Konferencja FSE jest wiodącą konferencją poświęconą kryptografii symetrycznej i kryptoanalizie, firmowana i organizowana przez International Association for Cryptology Research (IACR). Warto również dodać, że na tej samej konferencji zespół Adi Shamira zaprezentował pracę, w której wykorzystał (niezależnie) tę samą własność (stałe rundowe o niskich wagach Hamminga), w tym wypadku do poszukiwania kolizji dla zredukowanej funkcji Keccak.

W pracy [4] zostało przedstawione rozwinięcie ataku kostkami (ang. cube attack) i szczegółowa analiza tej klasy ataków dla algorytmów bazujących na permutacji Keccak-f. Atak kostkami, należący do rodziny technik algebraicznych, przedstawił Dinur i Shamir w 2009 roku [Dinur09], a wcześniej podobne pomysły można znaleźć w [Lai94] i [Vielhaber07]. Atak kostkami, jak kilka innych technik algebraicznych, stara się wykorzystać niski stopień wielomianów opisujących atakowany algorytm. To co jest szczególnie interesujące to fakt, że atakujący nie musi znać dokładnej specyfikacji kryptosystemu, który atakuje. Wystarczy, że wolno mu generować pary wiadomość-szyfrogram (w przypadku szyfrów) czy wiadomość-kod MAC w przypadku funkcji skrótu z kluczem. Nowatorskie podejście zaprezentowane w [4] bazuje na pomyśle by nie traktować algorytmu całkowicie jak „czarną skrzynkę" lecz starać się wykorzystać strukturalne własności analizowanej funkcji. Barierą w zastosowania ataku kostkowego do bardziej złożonych algorytmów (z większą liczbą rund) jest stopień wielomianu, którym opisane jest wyjście (np. szyfrogram). Zwykle wielomian ten rośnie wykładniczo od liczby rund. Bardziej wnikliwa analiza interakcji między zmiennymi wejściowymi (szczególnie w początkowych rundach) pozwoliła na dokładniejsze określenie stopnia wielomianu, co przełożyło się na złamanie większej liczby rund. Atak został przeprowadzony dla kilku algorytmów z rodziny Keccak tj. dla funkcji skrótu w trybie z kluczem, schematu szyfrowania z uwierzytelnieniem (Keyak v1) oraz szyfru strumieniowego. Wyniki te zaprezentowałem na konferencji EUROCRYPT w 2015 roku. (Konferencja EUROCRYPT jest jedną z flagowych konferencji organizowanych przez International Association for Cryptology Research.) Wyniki i badania dotyczące tej pracy przedstawiłem również na seminarium w Technical University of Denmark (DTU) na zaproszenie grupy Larsa Knudsena i Christiana Rechbergera — wiodącego zespołu kryptoanalitycznego w Europie. Warto także dodać, że publikacja ta stała się inspiracją dla innych badaczy, którzy dalej rozwinęli opisaną technikę lub zaaplikowali ją do innych algorytmów i scenariuszy ataku [Dong17], [Dobraunig15], [Zheng17].

Kolejna praca „Malicious SHA-3" [5] nie jest klasyczną kryptoanalizą lecz spojrzeniem na algorytm oczami projektanta i próbą takiej modyfikacji funkcji, która wprowadziłaby ukryte, „złośliwe" słabości. Ogólniej, złośliwy wariant algorytmu to taki, który posiada słabość zwaną tylną furtką (ang. backdoor). Osoba, która zna taką furtkę może łatwo manipulować lub nawet całkowicie zniszczyć bezpieczeństwo algorytmu. „Świętym Graalem" dla wszystkich agencji wywiadowczych jest posiadanie takich furtek, które byłyby niezwykle trudne do wykrycia, a jednocześnie łatwe w użyciu, z możliwością powszechnego stosowania. Dokumenty ujawnione przez Edwarda Snowdena pokazały, że NSA celowo umieściło tylną furtkę w standardowym generatorze liczb pseudolosowych Dual EC DRBG [Bernstein15]. Słabość ta pozwala poznać stan wewnętrzny generatora i tym samym

atakujący może przewidzieć przyszłe bity klucza. W tym kontekście badanie algorytmów kryptograficznych pod kątem złośliwego wariantu staje się nie tylko interesującym problemem badawczym ale i zagadnieniem mającym realne przełożenie na bezpieczeństwo funkcjonujących i przyszłych rozwiązań.

Dla funkcji SHA-3 zaproponowałem złośliwy wariant, w którym zmodyfikowane są stałe rundowe. Modyfikacje stałych rundowych inspirowane są kryptoanalizą rotacyjną oraz odmianą kryptoanalizy różnicowej dla algorytmu Keccak [Dinur13]. Odpowiednio dobrane stałe prowadzą do szybszych ataków na przeciwobraz (ang. preimage attack) i szybszego znajdowania kolizji niż wskazywałby atak przez paradoks dnia urodzin. Dodatkowo dla zaproponowanego wariantu zidentyfikowałem klasę słabych kluczy. Jeśli klucz należy do takiej klasy, możliwe staje się fałszerstwo kodu MAC.
Wyżej wymienione prace, które dotyczyły funkcji Keccak i standardu SHA-3 realizowałem w ramach grantu przyznanego z konkursu SONATA z Narodowego Centrum Nauki (grant nr UMO-2013/09/D/ST6/03918). W grancie pełniłem rolę kierownika i głównego wykonawcy.

Kryptoanaliza i projektowanie schematów szyfrowania z uwierzytelnianiem

Kolejne trzy prace z przedłożonego cyklu dotyczą kryptoanalizy schematów szyfrowania z uwierzytelnianiem (ang. authenticated encryption scheme). Taki algorytm powinien oferować dwie funkcjonalności: poufność i uwierzytelnianie przesyłanych danych. Schematy te budowane są najczęściej jako różne kombinacje szyfrów blokowych, szyfrów strumieniowych, kodów uwierzytelniania wiadomości i funkcji skrótu. Kilka rozwiązań zostało ustandaryzowanych w dokumentach ISO/ IEC, a jednym z najbardziej rozpowszechnionych jest AES-GCM [NIST07] - schemat bazujący na standardzie szyfrowania AES [Daemen02].

Dla wielu nowoczesnych aplikacji wymagania eksploatacyjne są bardzo wysokie i obowiązujące standardy schematów szyfrowania z uwierzytelnianiem (np. wspomniany już AES-GCM) zaczynają być niewystarczające. Dobrym przykładem jest VMware View, który jest protokołem komunikacyjnym stosowanym do zdalnego obsługiwania komputerów osobistych. Dokumentacja protokołu VMware zaleca przejście z AES-GCM na szybszy szyfr, by uzyskać zadowalający komfort pracy. Duże zainteresowanie i znaczenie algorytmów szyfrowania z uwierzytelnianiem odzwierciedla trwający konkursu CAESAR [Caesar14]. Konkurs rozpoczął się w 2014 i jego celem jest wyłonienie rodziny szyfrów, które będą konkurencyjne dla AES-GCM wg określonego kryterium (np. szybkość szyfrowania, skalowalność algorytmu, łatwość implementacji). Konkurs spotkał się z bardzo dużym odzewem ze strony społeczności naukowej, w pierwszej turze znalazło się 57 algorytmów z całego świata, w tym z wiodących ośrodków zajmujących się kryptologią. Poniżej omówione prace odzwierciedlają mój aktywny udział w tym obszarze badań, zarówno w zakresie projektowania algorytmów jak i kryptoanalizy.

Praca [6] jest projektem nowego szyfru z uwierzytelnianiem. Praca była realizowana w 8-osobowym, międzynarodowym zespole. Mój wkład w pracę to pomysł na algorytm, kryptoanaliza oraz kierowanie i koordynowanie prac poszczególnych członków zespołu. Na uwagę zasługuje fakt, że oprócz jednostek naukowo-badawczych (IPI PAN, George Mason

University USA, Queensland University of Technology, Australia) w zespole brali udział badacze pracujący w przemyśle tj. Krystian Matusiewicz (Intel) i Marcin Rogawski (Cadence Design System, San Jose, USA). Zaprojektowany szyfr ICEPOLE dedykowany jest przede wszystkim platformom sprzętowym takim jak układy FPGA i ASIC. W istocie ICEPOLE jest rodziną szyfrów parametryzowanych przez długość klucza (128 lub 256 bitów) i długość parametru „nonce" (od 0 do 128 bitów). Zakładany poziom bezpieczeństwa dla podstawowego wariantu to 128 bitów i założenie to poparte jest obszerną kryptoanalizą.
Szyfr ICEPOLE bazuje na konstrukcji „duplex" wprowadzonej przez projektantów funkcji Keccak [Bertoni11]. Zwykle sercem takiego rozwiązania jest permutacja i dla potrzeb szyfru ICEPOLE zaprojektowaliśmy nową permutację działającą na 1280-bitowym stanie. Korzystając z wcześniejszych doświadczeń przy analizie nieliniowego kroku funkcji Keccak, zaprojektowałem nowy S-box z dobrym poziomem bezpieczeństwa i niskim kosztem implementacyjnym. Zaproponowane rozwiązania dały w rezultacie szyfr o znakomitych parametrach wydajnościowych. ICEPOLE będzie bardzo dobrym wyborem w środowiskach gdzie wymagana jest wysoka przepustowość rzędu kilkudziesięciu gigabitów na sekundę. W testach z układem FPGA Virtex 6 podstawowa implementacja osiągnęła przepustowość 41 Gb/s co jest wynikiem 10-krotnie lepszym niż implementacja AES-GCM. Współczynnik „throughput-to-area" również jest kilkukrotnie lepszy od wyniku dla standardu AES-GCM. ICEPOLE prezentuje się również bardzo dobrze na tle algorytmów zgłoszonych do konkursu CAESAR. Dla układów FPGA, pod względem wydajności, plasuje się na trzecim miejscu (spośród 58 indeksowanych szyfrów) [Athena].
Projekt szyfru prezentowałem na konferencji CHES w 2014 roku. (Konferencja CHES jest najważniejszą konferencją dotyczącą kryptografii związanej z układami sprzętowymi, konferencja firmowana i organizowana przez International Association for Cryptology Research). Ponadto uzyskane wyniki i projekt szyfru przedstawiłem na seminarium w Bristol University (Wielka Brytania) na zaproszenie grupy Nigela Smarta. Warto również podkreślić, że algorytm spotkał się z żywym zainteresowaniem wielu grup kryptoanalitycznych, które przeprowadziły własną analizę ICEPOLE'a [Dobraunig15a, Dobraunig15b, Huang15, Jovanovic14, Sasaki15, Todo15]. Pozytywna weryfikacja przez strony trzecie uwiarygadnia projekt i zwiększa poziom zaufania do nowego rozwiązania.

W kolejnej publikacji [7] algorytmem poddanym kryptoanalizie był nowy schemat szyfrowania z uwierzytelnianiem MORUS. Szyfr ten został zaprojektowany przez dwóch badaczy z Nanyang University of Technology w Singapurze [Wu14]. Do analizy tego algorytmu posłużyły dwie techniki, to jest kryptoanaliza różnicowa i rotacyjna. Pod koniec lat 80-tych ubiegłego wieku Eli Biham i Adi Shamir przedstawili pierwszy raz publicznie nową metodę kryptoanalityczną nazwaną różnicową [Biham91]. Jednym z pierwszych zastosowań tej techniki był atak na szyfr DES ze zredukowaną liczbą rund. Istota kryptoanalizy różnicowej polega na śledzeniu różnic między dwiema wiadomościami, gdzie różnica zwykle definiowana jest jako operacja bitowa XOR. Atakujący posiada wiele par wiadomość-szyfrogram i na podstawie pewnych statystycznych prawidłowości w różnicach między szyfrogramami może uzyskać informacje na temat klucza. Jednym z wariantów tej techniki jest kryptoanaliza różnic wewnętrznych (ang. internal differentials), gdzie badane są zależności w obrębie pojedynczego stanu szyfru (a nie pary stanów). Ten wariant jest szczególnie przydatny dla szyfrów, które wykazują dużą symetrię w swojej budowie i właśnie takim szyfrem jest MORUS. Nowatorskim elementem naszej pracy jest wprowadzenie nowej odmiany ataku teoretycznego nazwanym przyspieszonym atakiem siłowym (ang. accelerated exhaustive search). Warto podkreślić, że atak nie ogranicza się tylko do jednego algorytmu (MORUSa w tym przypadku), lecz może być stosowany do

innych funkcji, nawet o zupełnie innej budowie. W pracy zweryfikowałem również założenie autorów MORUSa, że brak stałych rundowych nie jest przeszkodą w osiągnięciu wysokiego poziomu bezpieczeństwa szyfru. Przeprowadzona analiza potwierdza to założenie i zgadza się z tezą autorów, że szyfr jest nie tylko bardzo wydajny ale i bezpieczny.

Następną pracą [8] z przedłożonego cyklu stanowi analiza sześciu szyfrów, które brały (lub wciąż biorą) udział w konkursie CAESAR. Praca była realizowana w 6-osobowym międzynarodowym zespole (IPI PAN, Queensland University of Technology z Australii, Uniwersytet Karola w Pradze oraz Nanyang University of Technology w Singapurze). Byłem pomysłodawcą i kierownikiem całego projektu, a także uczestniczyłem w implementowaniu ataków. W pracy tej szczególna uwaga została poświęcona klasie szyfrów bazujących na konstrukcji zwanej funkcją gąbkową (ang. sponge function) i jej „siostrzanym" wariancie — konstrukcji duplex.
Słowo „konstrukcja" należy tutaj rozumieć jako sposób połączenia i korzystania z mniejszych kryptograficznych algorytmów, w tym wypadku kryptograficznie silnej permutacji. Konstrukcja gąbkowa i jej warianty mogą być użyte do projektowania wielu różnych algorytmów takich jak funkcje skrótu, szyfry strumieniowe, generatory pseudolosowe czy też właśnie schematy szyfrowania z uwierzytelnianiem. Z tej ostatniej rodziny zostały przeanalizowane ASCON [Dobraunig14], ICEPOLE [Morawiecki14], NORX [Aumasson14] i Ketje [Bertoni14]. Konstrukcja gąbkowa/duplex wykorzystuje permutację określoną dwoma parametrami: przepływnością (ang. bitrate) i pojemnością (ang. capacity). Suma tych dwóch parametrów daje rozmiar permutacji. Dobierając odpowiednio przepływność i pojemność użytkownik ma możliwość określenia kompromisu między szybkością a bezpieczeństwem algorytmu. Z większą przepływnością algorytm będzie działał szybciej ale z mniejszym marginesem bezpieczeństwa.
Przeprowadzone badania pozwoliły wypełnić lukę w kryptoanalizie pięciu szyfrów, które wcześniej nie były wnikliwie analizowane z użyciem testerów SAT. Pełne wersje tych algorytmów okazały się zbyt silne dla kryptoanalizy logicznej, co potwierdza duży poziom bezpieczeństwa i wiarygodności tych rozwiązań. Okazało się jednak, że dla zredukowanych wersji lub wariantów ze zmodyfikowanymi parametrami przepływności i pojemności, ataki są możliwe. Dzięki tym wynikom precyzyjniej można określić margines bezpieczeństwa dla analizowanych szyfrów co w kontekście konkursu CAESAR i ogólnej potrzeby wydajniejszych rozwiązań ma duże znaczenie.
Prace poświęcone schematom szyfrowania z uwierzytelnieniem realizuję w ramach grantu uzyskanego z Narodowego Centrum Nauki z konkursu OPUS (grant nr UMO-2014/15/B/ST6/05130). Byłem pomysłodawcą i głównym redaktorem wniosku, pełnię również rolę głównego wykonawcy grantu.

Kryptoanaliza szyfrów blokowych dedykowanych lekkiej kryptografii

Ostatnie dwie prace [9, 10] poświęcone są kryptoanalizie szyfrów blokowych, które były projektowane z myślą o tzw. lekkiej kryptografii (ang. lightweight cryptography). Aplikacje takie jak znaczniki RFID, bezprzewodowe sieci czujników czy spersonalizowana, precyzyjna medycyna zrodziły potrzebę kryptograficznych rozwiązań, które muszą dobrze radzić sobie w środowiskach o ograniczonych możliwościach pamięciowo-obliczeniowych.

W publikacji [9] przedstawiłem kryptoanalizę szyfru PRINCE i jego zredukowanych wariantów. Szyfr ten został przedstawiony na konferencji Asiacrypt'12 i jest owocem współpracy naukowców z firmą NXP Semiconductors. PRINCE był zaprojektowany z myślą o zastosowaniach gdzie bardzo małe czasowe opóźnienie przy szyfrowania i natychmiastowy czas reakcji jest niezwykle ważny. Dobrym przykładem może być szyfrowana transmisja podczas jazdy na autostradzie, gdzie „w locie" sprawdzane są winiety samochodów dostawczych.
Mój główny wynik z tej pracy to atak na 7-rundowy wariant szyfru, gdzie użyłem kryptoanalizy różnicowej wyższego rzędu (ang. higher-order differentials). Atak ten prowadzi do odzyskania tajnego klucza a złożoność czasowa wynosi 2^{57}. Dodatkowo przeprowadziłem atak bazujący na kryptoanalizie sumacyjnej (ang. integral analysis) dla 6-rundowego wariantu. Atak ten ma praktyczną złożoność czasową i został zaimplementowany na pojedynczym komputerze klasy PC.
W ostatnich kilku latach szyfr PRINCE był szeroko analizowany przez społeczność akademicką. Jednakże większość ataków ma charakter teoretyczny to znaczy złożoność czasowa lub ilość danych wymaganych przy ataku przekracza znacznie możliwości współczesnych komputerów. By zachęcić do bardziej praktycznych analiz (nawet kosztem mniejszej liczby rund), autorzy szyfru PRINCE ogłosili konkurs na ataki odzyskujące tajny klucz, gdzie złożoność czasowa nie może przekroczyć 2^{64} [Challenge]. Wyniki z mojej publikacji wraz z dostarczoną implementacją zwyciężyły w jednej z kategorii konkursu.

Drugą pracą [10] poświęconą „lekkim" szyfrom blokowym jest analiza szyfru SPECK [Beaulieu13]. Współautorami analizy są doktoranci z Instytutu Podstaw Informatyki, z którymi realizuje grant z konkursu OPUS i pełnię rolę ich opiekuna naukowego. SPECK został zaprojektowany przez badaczy z National Security Agency (NSA) w Stanach Zjednoczonych. Konstrukcja algorytmu jest bardzo zbliżona do innego szyfru Threefish, który jest główną składową funkcji skrótu Skein [Schneier]. SPECK został zaprojektowany tak by miał wysoką wydajność zarówno na platformach programowych jak i sprzętowych, ale szczególna uwagę poświęcono optymalizacji na potrzeby mikrokontrolerów. SPECK należy do rodziny szyfrów ARX czyli wykorzystuje tylko trzy proste operacje: dodawanie, rotacje bitów i operacje XOR. Zaletą tej rodziny algorytmów jest prostota i wydajność, ale z kolei kryptoanaliza jest trudniejsza i techniki typowe dla algorytmów takich jak AES nie dają się bezpośrednio zastosować. W szczególności sposób przeprowadzania kryptoanalizy różnicowej jest inny gdyż w algorytmach klasy ARX nie ma typowych S-boxów, a źródłem nieliniowości jest operacja dodawania modulo.
W pracy zaproponowano nową metodę szukania ścieżek różnicowych a inspiracją był algorytm Nested Monte Carlo Search używany do jednoosobowych gier. Pomysł bazuje na tym by traktować budowanie ścieżek różnicowych również jako jednoosobową grę i użyć randomizowanej heurystyki do znajdowania coraz lepszych rozwiązań. Pomysł został zaimplementowany i zweryfikowany na szyfrze SPECK32. Wyniki dla tego wariantu szyfru SPECK są na poziomie najlepszego rezultatu opublikowanego w [Biryukov14]. By uzyskać zadowalające rezultaty dla szyfrów o większym rozmiarze bloku potrzeba wzmocnić losowy sposób wybierania ścieżek. Ten problem stanowi aktualne zadanie badawcze.
Mój wkład w pracę poświęconą szyfrowi SPECK to pomysł opisanego podejścia do kryptoanalizy różnicowej i redakcja publikacji. Implementację w języku Python wykonali doktoranci Ashutosh Dhar Dwivedi i Sebastian Wójtowicz.

5. Omówienie pozostałych osiągnięć naukowo-badawczych

W pierwszym okresie swojej pracy badawczej (do uzyskania stopnia doktora) zajmowałem syntezą logiczną funkcji boolowskich. Doświadczenia i warsztat opanowany z tego okresu wykorzystałem w dwóch pracach dotyczących kryptoanalizy logicznej [1,2].
W szczególności prace nad dekompozycją funkcji boolowskich i generowaniem prostych równań okazały się bardzo pomocne w stworzeniu zautomatyzowanego generatora formuł dla testerów SAT. Prace badawcze z tego okresu realizowałem w ramach międzynarodowego grantu współfinansowanego przez Agency for Science, Technology and Research A*STAR w Singapurze.

Poniżej chciałbym pokrótce przybliżyć kilka prac, które dotyczą kryptoanalizy a nie znalazły się w przedłożonym cyklu publikacji.

W pracy [Dhar17] prowadziłem badania (wraz z doktorantami Sebastianem Wójtowiczem i Ashutoshem Dharem) nad schematem szyfrowania z uwierzytelnianiem SCREAM. Szyfr ten został zaprojektowany ze szczególnym uwzględnieniem bezpieczeństwa sprzętowego (ataki typu side-channel). Przeprowadziliśmy szereg ataków kryptoanalitycznych na zredukowane warianty szyfru SCREAM, a uzyskane wyniki zostały zaprezentowane na konferencji SECRYPT w 2017 roku w Madrycie.

Kryptograficznie silna funkcja skrótu powinna być odporna na atak na przeciwobraz, tj. dla zadanego skrótu atakujący nie powinien móc łatwo odnaleźć wiadomości odpowiadającej danemu skrótowi. W pracy [Morawiecki13] został przedstawiony teoretyczny atak na przeciwobraz dla zredukowanych wariantów funkcji Keccak. Zaproponowałem nowatorskie wykorzystanie ścieżek różnicowych do znajdowania przeciwobrazów. Przedstawiona technika może być zastosowana również do innych algorytmów, szczególnie dobrze nadaje się do funkcji o słabej dyfuzji (rozpraszaniu) informacji pomiędzy bitami stanu. W drugiej pracy [Chang14] podejmującej temat ataku na przeciwobraz wykorzystano algebraiczne własności permutacji Keccak-f oraz strukturalne własności tej funkcji. Uzyskany wynik to atak na 9 rund, co jest obecnie najlepszym teoretycznym atakiem na przeciwobraz dla funkcji Keccak/SHA3. Praca ta została wykonana we współpracy z naukowcami z Indraprastha Institute of Information Technology w Delhi w Indiach. Wyniki zostały przedstawione na konferencji „SHA-3 Workshop 2014” w Santa Barbara w Stanach Zjednoczonych.

Kolejna praca dotyczy konstrukcji „sponge/duplex”, która pozwala, między innymi, na budowę schematów szyfrowania z uwierzytelnianiem. Jednakże pierwsza wersja architektury duplex nie wspierała przetwarzania równoległego. Wraz z Józefem Pieprzykiem zmierzyliśmy się z tym problemem w pracy [Morawiecki13a], gdzie zaproponowaliśmy schemat szyfrowania i uwierzytelniania równoległego dla algorytmów bazujących na konstrukcji duplex. Doświadczenia z tej pracy wykorzystałem później podczas projektu szyfru ICEPOLE [Morawiecki14].

Ostatnia praca, którą chciałem przybliżyć to propozycja wariantu ataku kostkowego dedykowanego atakom z bocznym kanałem (ang. side-channel attack) [Morawiecki15]. Ten

rodzaj ataku bazuje na informacjach uzyskanych z fizycznej implementacji danego kryptosystemu. Urządzenia kryptograficzne często niezamierzenie udostępniają dodatkowe informacje (tzw. boczny kanał), które mogą być wykorzystywane w tego rodzaju atakach. Taką informacją może być promieniowanie elektromagnetyczne, czas wykonywania obliczeń, zużycie prądu. W typowym scenariuszu atakujący ma dostęp do części informacji, np. wartości rejestrów stanu na pewnym etapie przetwarzania. W pracy zaproponowałem atak, który zakłada „wyciek" po kilku rundach działania szyfru. Mój główny wkład to metoda ataku, która jest bardziej odporna na błędy pomiary — niekorzystne i powszechne zjawisko w atakach typu „side-channel". Symulacja ataku została przeprowadzona dla funkcji Keccak działającej w trybie MAC przy założeniu, że implementacja jest na 8-bitowym procesorze, a wyciek następuje podczas ładowania danych z pamięci do jednostki arytmetyczno-logicznej.

Wszystkie pozostałe osiągnięcia naukowo-badawcze, dydaktyczne, popularyzatorskie i inne zostały opisane w załączniku „Wykaz dorobku w naukach technicznych dla wniosku habilitacyjnego".

Literatura

[Athena] ATHENa: Automated Tools for Hardware EvaluatioN, https://cryptography.gmu.edu/athenadb/fpga_auth_cipher/rankings_view

[Aumasson] Aumasson J-P. et al., SHA-3 proposal BLAKE, http://www.131002.net/blake/

[Aumasson14] Aumasson J-P., Jovanovic P., Neves S.: NORX: parallel and scalable aead. In European Symposium on Research in Computer Security, pages 19–36. Springer, 2014

[Beaulieu13] Beaulieu R., Shors D., Smith J., Treatman-Clark S., Weeks B., Wingers L.,: The SIMON and SPECK families of lightweight block ciphers, IACR Cryptology ePrint Archive, vol. 2013, p. 404, 2013.

[Bernstein15] Bernstein, D.J.,Lange, T.,Niederhagen, R., Dual EC: A Standardized Back Door. Cryptology ePrint Archive, Report 2015/767 (2015), http://eprint.iacr.org

[Bertoni11] Bertoni, G., Daemen, J., Peeters, M., Assche, G.V.: Duplexing the sponge: single-pass authenticated encryption and other applications. Cryptology ePrint Archive, Report 2011/499 (2011)

[Bertoni14] Bertoni G., Daemen J., Peeters M., Van Assche G., Van Keer R.: CAESAR submission: KETJE v2 . http://ketje.noekeon.org

[Biham91] Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptology 4(1), 3–72 (1991)

[Biryukov14] Biryukov A., Velichkov V.: Automatic search for differential trails in ARX ciphers, in Topics in Cryptology - CT-RSA 2014 - The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, February 25-28, 2014. Proceedings, 2014, pp. 227–250.

[Caesar14] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, http://competitions.cr.yp.to/caesar.html

[Challenge] The PRINCE Challenge https://www.emsec.rub.de/research/research_startseite/prince-challenge

[Chang14] Chang D., Kumar A., Morawiecki P., Kumar Sanadhya S.: 1st and 2nd Preimage Attacks on 7, 8 and 9 Rounds of Keccak-224, 256, 384, 512., SHA-3 Workshop 2014, Santa Barbara, USA

[Contest] The Keccak Crunchy Crypto Collision and Pre-image Contest, https://keccak.team/crunchy_contest.html

[Daemen02] Daemen, J., Rijmen, V.: The Design of Rijndael: AES - The Advanced Encryption Standard. Information Security and Cryptography, Springer (2002)

[Dhar17] Dhar A., Morawiecki P., Wójtowicz S.: Differential-linear and Impossible Differential Cryptanalysis of Round-reduced Scream, Proceedings of SECRYPT 2017, Madrid 2017

[Dinur09] Dinur, I., Shamir, A.: Cube attacks on tweakable black box polynomials. In: EUROCRYPT. pp. 278–299 (2009)

[Dinur13] Dinur, I., Dunkelman, O., Shamir, A.: Collision Attacks on Up to 5 Rounds of SHA-3 Using Generalized Internal Differentials. In: Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers. pp. 219–240 (2013)

[Dobraunig14] Dobraunig C., Eichlseder M., Mendel F., Schläffer M.: ASCON A Family of Authenticated Encryption Algorithms. http://ascon.iaik.tugraz.at

[Dobraunig15] Dobraunig C., Eichlseder M., Mendel F, Schläffer M.: Cryptanalysis of Ascon. CT-RSA 2015.

[Dobraunig15a] Dobraunig C., Eichlseder M., Mendel F.: Forgery Attacks on round-reduced ICEPOLE-128. Selected Areas Of Cryptography 2015.

[Dobraunig15b] Dobraunig C., Eichlseder M., Mendel F.: Heuristic Tool for Linear Cryptanalysis with Applications to CAESAR Candidates. ASIACRYPT 2015.

[Dong17] X. Dong, Z. Li, X. Wang and L. Qin, Cube-like Attack on Round-Reduced Initialization of Ketje Sr, FSE 2017

[Gauravaram] Gauravaram P. et al., Grøstl—a SHA-3 candidate, http://www.groestl.info

[Huang15] Huang T., Tjuawinata I., Wu H.: Differential-Linear Cryptanalysis of ICEPOLE. Fast Software Encryption 2015.

[Jovanovic14] Jovanovic P., Luykx A., Mennink B.: Beyond 2^{c/2} Security in Sponge-Based Authenticated Encryption Modes. ASIACRYPT 2014.

[Keccak] Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Keccak Sponge Function Family Main Document, http://keccak.noekeon.org/Keccak-main-2.1.pdf

[Khovratovich10] Khovratovich, D., Nikolić, I.: Rotational cryptanalysis of ARX. In: Proceedings of the 17th international conference on Fast software encryption. pp. 333–346. LNCS, Springer-Verlag (2010)

[Lai94] Lai, X.: Higher order derivatives and differential cryptanalysis. In: Blahut, R., Costello, DanielJ., J., Maurer, U., Mittelholzer, T. (eds.) Communications and Cryptography, The Springer Inter- national Series in Engineering and Computer Science, vol. 276, pp. 227–233. Springer US (1994)

[Massaci99] Massacci, F.: Using Walk-SAT and Rel-SAT for cryptographic key search. In: In Proceedings of the International Joint Conference on Artificial Intelligence. pp. 290–295 (1999)

[Morawiecki10] Morawiecki, P., Srebrny, M.: A SAT-based preimage analysis of reduced KECCAK hash functions. In: Second SHA-3 Candidate Conference, Santa Barbara (2010)

[Morawiecki13] Morawiecki P., Pieprzyk J., Srebrny M., Straus M.: Preimage attacks on the round-reduced Keccak with the aid of differential cryptanalysis, Cryptology ePrint Archive, Report 2013/561

[Morawiecki13a] Morawiecki P., Pieprzyk J.: Parallel authenticated encryption with the duplex construction., Cryptology ePrint Archive, Report 2013/658

[Morawiecki14] Morawiecki P., Gaj K., Homsirikamol E., Matusiewicz K., Pieprzyk J., Rogawski M., Srebrny M., Wójcik M.: ICEPOLE: High-Speed, Hardware-Oriented Authenticated Encryption. In Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings, pages 392–413, 2014

[Morawiecki15] Morawiecki P., Pieprzyk J., Srebrny M., Straus M.: Applications of Key Recovery Cube-attack-like, Cryptology ePrint Archive, Report 2015/1009

[NIST07] National Institute of Standards and Technology: Recommendations for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST special publication 800-38D (November 2007)

[Sasaki15] Sasaki Y., Yasuda K.: How to Incorporate Associated Data in Sponge-Based Authenticated Encryption. CT-RSA 2015.

[Schneier] Schneier B. et al., The Skein Hash Function Family, http://www.skein-hash.info/sites/default/files/skein1.1.pdf

[Todo15] Todo Y.: Structural Evaluation by Generalized Integral Property. EUROCRYPT 2015.

[Vielhaber07] Vielhaber, M.: Breaking ONE.FIVIUM by AIDA an Algebraic IV Differential Attack. Cryptology ePrint Archive, Report 2007/413 (2007)

[Wang05] Wang, X., Yin, Y.L., Yu, H.: Finding Collisions in the Full SHA-1. In: Crypto. LNCS, vol. 3621, pp. 17–36. Springer (2005)

[Wu] Wu, H.: Hash Function JH, http://www3.ntu.edu.sg/home/wuhj/research/jh

[Wu14] Wu H., Huang T.: The Authenticated Cipher MORUS. https://competitions.cr.yp.to/caesar-submissions.html

[Zheng17] Zheng Li, Xiaoyang Dong, Xiaoyun Wang. Conditional Cube Attack on Round-Reduced ASCON. IACR Transactions on Symmetric Cryptology 2017(1), 175–202.