# Streszczenie

W pracy podjęto zagadnienie kryptoanalizy funkcji skrótu Keccak, przyjętego w sierpniu 2015 roku jako amerykański standard SHA-3 (od ang. Secure Hash Algorithm). Kryptograficzne funkcje skrótu są podstawowym elementem wielu współczesnych algorytmów stosowanych m.in. w podpisie elektronicznym, uwierzytelnianiu danych, przechowywaniu haseł. Algorytm funkcji skrótu jest jednokierunkową funkcją pseudolosową zamieniającą zadany ciąg danych o dowolnej długości na ciąg o z góry ustalonej długości, np. 256 bitów, spełniając określone wymagania bezpieczeństwa.

Szeroko rozpowszechnione do niedawna funkcje skrótu, takie jak SHA-1 bazujące na konstrukcji podobnej do MD5, okazały się podatne na ataki kryptoanalityczne. Reakcją na ten stan rzeczy było ogłoszenie przez amerykański National Institute of Standards and Technology (NIST) otwartego konkursu na nową funkcję skrótu. Ostatecznie zwycięzcą został algorytm Keccak. Algorytm ten jest skonstruowany na podstawie całkowicie nowej architektury nazwanej funkcją gąbkową (ang. sponge function) - nowego podejścia do tworzenia funkcji skrótu. Składa się z etapu wchłaniania kolejnych bloków danych wejściowych i mieszaniu ich, po czym następuje etap wyciskania skrótu. Intuicyjnie przypominające gąbkę.

Konstrukcja ta ma wszechstronne zastosowanie w budowaniu systemów kryptograficznych, wymaga zatem podjęcia szerokich prac badawczych. Celem niniejszej pracy jest podjęcie badań kryptoanalitycznych nad bezpieczeństwem funkcji gąbkowej Keccak.

Rozprawa zaczyna się od wprowadzenia zagadnień niezbędnych do prezentacji wyników badawczych. Przedstawione są podstawowe informacje dotyczące metod konstrukcji funkcji skrótu i znane dotąd metody ataków. W tym prezentacja specyfikacji funkcji gąbkowej Keccak i możliwych zastosowań, m.in. jako szyfru strumieniowego. Przedstawiony jest też Keyak - szyfr z uwierzytelnianiem (ang. authenticated encryption), opracowany przez twórców Keccaka na algorytmie funkcji gąbkowej Keccak. Opisano także zasady ataku kostkami (ang. cube attack) i ataku sumacyjnego.

Główną cześć rozprawy stanowią wyniki ataku kostkami i analizy sumacyjnej na różne konfiguracje i zastosowania algorytmu Keccak, m.in. szyfru strumieniowego, kodu uwierzytelnienia wiadomości i szyfru z uwierzytelnianiem Keyak. Uzyskano rezultaty istotne z punktu postawionego celu pracy i hipotez badawczych, a wybrane wyniki zostały przedstawione na renomowanych konferencjach SHA-3 2014 Workshop oraz Eu-

rocrypt 2015.

Najważniejszym wynikiem jest atak kostkami o praktycznej złożoności obliczeniowej na 6-rundowy wariant funkcji gąbkowej Keccak działającej w trybie szyfru strumieniowego. Klasyczny atak kostkami został tu wzbogacony przez wykorzystanie strukturalnych i algebraicznych własności permutacji Keccak. Drugi ważny wynik to wariant ataku kostkami oparty na paradygmacie „dziel i zwyciężaj", gdzie klucz odzyskiwany jest w kilku etapach. Podejście to zaowocowało teoretycznymi atakami na 7- i 8-rundowe warianty funkcji gąbkowej działającej w trybie szyfru strumieniowego oraz szyfrowania z uwierzytelnianiem algorytmem Keyak. Wymienione wyniki pozostają do dziś najlepsze na świecie.