Streszczenie

Ataki algebraiczne są rodzajem kryptoanalizy, polegającej na przedstawieniu szyfru za pomocą układu równań, a następnie rozwiązaniu tego układu. Niestety, ataki te są efektywne tylko dla szyfrów o prostych strukturach algebraicznych, tzn. z niskim stopniem algebraicznym funkcji rundy. W przypadku dobrze zaprojektowanego szyfru, trudno jest znaleźć równania niskiego stopnia, a złożoność obecnie stosowanych w atakach algebraicznych algorytmów maleje, gdy układ jest nadokreślony. Mimo to, algorytmy te nie umożliwiają przeprowadzenia ataku w czasie krótszym, niż atak pełnego przeszukiwania. Dlatego też, w niniejszej rozprawie wykorzystano ideę ataków algebraicznych, jednak zamiast konstruować układy nadokreślone, skupiono się na konstruowaniu układu równań, umożliwiającego otrzymanie możliwie jak najmniejszego docelowego problemu w postaci QUBO, rozwiązywanego przy użyciu wyżarzania kwantowego. Głównym celem niniejszej rozprawy było dostosowanie znanego modelu transformacji układu równań do postaci problemu optymalizacyjnego, rozwiązywanego za pomocą wyżarzania kwantowego, do wykorzystania w atakach algebraicznych na szyfry blokowe. W pracy wzięto również pod uwagę realizację procesu rozwiązywania problemów optymalizacyjnych za pomocą komputera kwantowego D-Wave, który został wybrany jako narzędzie do przeprowadzenia ataków algebraicznych.

Podczas przeprowadzonych badań dla przykładowych algorytmów trzech najpopularniejszych typów struktur szyfrów blokowych (SPN, ARX oraz Feistel) udało się znaleźć układy równań, dające możliwie najmniejszy rozmiar problemu w postaci QUBO. Dla standardu AES skupiono się na warstwie nieliniowej i znaleziono efektywny układ, opisujący skrzynkę podstawieniową, co umożliwiło uzyskanie o 70% mniejszą liczbę zmiennych binarnych w ostatecznym problemie QUBO, w porównaniu do dotychczas opublikowanych wyników. Dla szyfru Speck przedstawiono dwie różne metody konstruowania układu równań nad $\mathbb{Z}_{2^n}$, skupiając się na realizacji operacji szyfru w $\mathbb{Z}_{2^n}$ oraz kolejności ich wykonywania. Ponieważ macierz uzyskanego problemu optymalizacyjnego była gęstsza niż w przypadku algorytmu AES, to dla tego samego szyfru Speck przedstawiono sposób konstruowania układu równań nad $\mathbb{F}_2$. Analizując różne struktury algebraiczne, nad którymi wyznaczone zostały równania opisujące dany szyfr blokowy pokazano, że struktura macierzy ostatecznego problemu optymalizacyjnego ma również wpływ na szybkość uzyskania rozwiązania za pomocą komputera kwantowego D-Wave. Dla

szyfru Simon, ze względu na liniowość operacji w algorytmie generowania kluczy rundowych, przedstawiono dwa sposoby konstruowania układu równań, w zależności od sposobu reprezentacji bitów kluczy rundowych. Dodatkowo, dla małych instancji analizowanych szyfrów blokowych przeprowadzono atak praktyczny, na dostępnych zasobach komputera kwantowego D-Wave. W rozprawie przedstawiono również szacowane złożoności zaproponowanego ataku dla różnych wariantów i parametrów rozpatrywanych szyfrów blokowych. W wyniku przeprowadzonych badań, dla niektórych wariantów uzyskano szacunkowe złożoności mniejsze niż dla najlepszych aktualnie znanych ataków klasycznych na te szyfry.