Warszawa, 15.05.2023

Recenzja rozprawy doktorskiej „Ataki algebraiczne na szyfry blokowe z wykorzystaniem wyżarzania kwantowego" autorstwa Elżbiety Burek

Tematyka rozprawy

Tematyka rozprawy dotyczy kryptoanalizy algebraicznej ze szczególnym uwzględnieniem metody wyżarzania kwantowego przeprowadzonego na komputerze udostępnianym przez firmę D-Wave. Autorka skoncentrowała swoją uwagę na trzech wiodących rodzinach szyfrów: SPN (substitution-permutation network), ARX (add, rotate, xor), oraz szyfrach Feistela. Wybrani reprezentanci poszczególnych rodzin to odpowiednio: standard AES, szyfr Speck i szyfr Simon.

Charakterystyka rozprawy

Poniżej przedstawiam ogólną charakterystykę rozprawy. Głównym celem rozprawy postawionym przez Autorkę jest „dostosowanie modelu transformacji układu równań do postaci problemu optymalizacyjnego, rozwiązywanego za pomocą wyżarzania kwantowego [...]". Układy równań podlegające transformacji pochodzą z opisu algebraicznego atakowanych szyfrów blokowych. Liczba zmiennych w układach równań jest kluczową wartością przekładającą się bezpośrednio na oszacowanie kosztu ataku przy pomocy wyżarzania kwantowego.

Do realizacji postawionego celu wyznaczono cztery zadania szczegółowe:

1) Analiza implementacji procesu wyżarzania kwantowego w komputerze firmy D-Wave

2) Transformacja układu równań wielomianowych do problemu optymalizacyjnego w postaci QUBO
3) Analiza wybranych szyfrów blokowych w kontekście nakreślonego celu
4) Przeprowadzenie ataku na komputerze D-Wave dla zredukowanych wersji szyfrów

W pracy brakuje tezy (hipotezy) badawczej, którą Doktorantka mogłaby postawić na wstępie i próbować ją weryfikować przeprowadzając badania.

Struktura rozprawy

Rozprawa podzielona jest na 7 rozdziałów.

W pierwszym rozdziale Autorka przedstawia najbardziej znane ataki algebraiczne w tym bazy Grobnera, różne warianty linearyzacji oraz idee używania SAT-solverów.

Rozdział drugi koncentruje się na obliczeniach kwantowych i kwantowym komputerze D-Wave. Początek tego rozdziału stanowi ogólne wprowadzenie do kwestii obliczeń kwantowych, z naciskiem na adiabatyczny model obliczeń kwantowych oraz kwantowe wyżarzanie. W drugiej części przedstawiono charakterystykę komputera kwantowego D-Wave, omawiając sposób wdrożenia i realizacji procesu kwantowego wyżarzania na tym urządzeniu. Dodatkowo szczegółowo omówiono proces rozwiązywania problemów optymalizacyjnych przy użyciu komputera D-Wave.

W rozdziale trzecim przedstawiono proponowany model przekształcenia układu równań wielomianowych, które przekształcają dowolny szyfr blokowy w problem optymalizacyjny QUBO. Przedyskutowano kolejne etapy transformacji oraz metody wykorzystane do ich realizacji. Na zakończenie rozdziału opisano wymagania, które musi spełniać układ opisujący szyfr blokowy, aby uzyskać problem w postaci QUBO o jak najmniejszych wymiarach.

W kolejnym rozdziale omówiono standard AES w odniesieniu do reprezentacji go za pomocą układu równań, który po przekształceniu do problemu QUBO pozwoli na uzyskanie jak najmniejszego rozmiaru problemu optymalizacyjnego. Szczególny nacisk położono na odkrycie efektywnego układu dla skrzynki podstawieniowej.

W rozdziale piątym znajdziemy analizę szyfru klasy ARX, konkretnie szyfru Speck, pod kątem problemu QUBO. Rozpatrywane są skrócone warianty szyfru.

Kolejna rozdział ma bardzo podobną strukturę do dwóch poprzednich tyle, że analizie poddany jest szyfr Simon reprezentujący rodzinę szyfrów blokowych o strukturze Feistela.

Rozprawa zakończona jest kilkustronicowym podsumowaniem, gdzie zebrane są główne wyniki oraz nakreślone dalsze kierunki badań.

Uwagi

Tematyka pracy jest interesująca. Na pewno nie jest to wyeksploatowany kierunek badań i wraz ze wzrostem możliwości komputerów kwantowych rola takich prac może wzrosnąć. Dwie najważniejsze publikacje zawierające wyniki prac to:

- Elzbieta Burek, Michal Wronski, Krzysztof Mank, Michal Misztal: „Algebraic Attacks on Block Ciphers Using Quantum Annealing", IEEE Transactions on Emerging Topics in Computing, Volume 10, 2022

- Elzbieta Burek, Michal Wronski: Quantum Annealing and Algebraic Attack on Speck Cipher. ICCS (4) 2022

Oba miejsca publikacji są uznanymi pozycjami (lista A, 140 pkt).

To co może być nieco zniechęcające to fakt, że wyniki kryptoanalityczne wciąż zatrzymują się na poziomie mocno zredukowanych wariantów, mimo użycia wyżarzania kwantowego. Przeprowadzone ataki z wykorzystaniem komputera firmy D-Wave mają charakter bardziej dydaktyczny, klucze są bardzo krótkie (np. 8 bitów dla szyfru Simon).
Aby oszacować złożoność ataku z wykorzystaniem wyżarzania kwantowego, Autorka korzysta z heurystycznego oszacowania problemu QUBO ze zmiennymi binarnymi.
Trudno ocenić na ile dobre jest taki oszacowanie przy tak małych rozmiarach problemów, które aktualnie można zaatakować z pomocą komputera D-Wave. Nie jest to zarzut, a raczej obserwacja, że zakładane złożoności są nieco spekulatywne.

Praca składa się z ponad 200 stron. Myślę, że bez straty na przekazie najważniejszych treści, można by pominąć szczegóły techniczne związane z topologią komputera D-Wave i szczegółami jego funkcjonowania. W zamian chętnie bym widział dokładniejszy opis metod generowania równań z Rozdziału 4. Schematy graficzne mogłyby zostać wzbogacone pseudokodem czy innym bardziej formalnym opisem proponowanego algorytmu.

Przy podawaniu wyników kryptoanalitycznych warto podać złożoność ataków. Autorka podaje tylko liczbę rund, które teoretycznie da się złamać przy pomocy zaproponowanego algorytmu.

Znalazłem w pracy kilka drobnych niedociągnięć natury językowej. Niektóre sformułowania są niezręczne, przykładowo „analizę przedstawienia szyfru blokowego typu ARX". Słowo analiza jest nadużywane w tekście rozprawy.

Konkluzja

Wartość merytoryczna pracy zdecydowanie przewyższa wymienione mankamenty. Uważam, że złożona rozprawa mgr Elżbiety Burek spełnia wymagania ustawowe i zwyczajowe stawiane pracom doktorskim i może stanowić podstawę nadania stopnia doktora w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie informatyka techniczna i telekomunikacja.

Piotr Kowiecki

Piotr Kowiecki

15.05.2023