dr hab. Bartłomiej Gardas
Instytut Informatyki
Teoretycznei i Stosowanei PAN
ul. Bałtycka 5, 44-100 Gliwice

Katowice, 10 maja 2023r.

Recenzja rozprawy doktorskiej Pani kpt. mgr inż. *Elżbiety BUREK*:
Ataki algebraiczne na szyfry blokowe z wykorzystaniem wyżarzania kwantowego

1 Uwagi wstępne

Forma drukowana prezentowanej rozprawy obejmuje 207 stron. Praca napisana jest w języku polskim i zwiera: • stronę tytułową • spis treści • wprowadzenie • 7 rozdziałów oraz • wykaz literatury. Promotorem oraz promotorem pomocniczym są Panowie: dr hab. Marek KOJDECKI oraz dr inż. Michał WROŃSKI z Wydziału Cybernetyki (Instytutu Matematyki i Kryptologi) Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego.

Praca zawiera wyniki opublikowane wcześniej przez Autorkę w formie artykułów naukowych:

A1 E. Burek, M. Wroński, K. Mańk, M. Misztal. Algebraic attacks on block ciphers using quantum annealing. IEEE Transactions on Emerging Topics in Computing, 10(2):678–689, 2022.

A2 E. Burek, M. Wroński. Quantum annealing and algebraic attack on speck cipher. Computational Science – ICCS 2022. Lecture Notes in Computer Science, **13353**, 143-149 (2022).

Pierwsze z czasopism ma wskaźnik wpływu (*ang.* impact factor) wynoszący **IF = 6.595** oraz **140** punktów ministerialnych (zgodnie ministerialną listą czasopism punktowanych), drugie natomiast **IF = 3.976** oraz **140** pkt. Nie znalazłem innych opublikowanych prac naukowych, których Pani kpt. mgr inż. Elżbieta BUREK jest autorem lub współautorem.

W wszystkich pracach doktorantka jest wiodącą autorką. Zwyczajowo przyjąć więc można, iż jej wkład w uzyskanie (oraz opublikowanie) wyników badań naukowych jest znaczący, a bez jej udziału nie byłoby to możliwe.

2 Przedmiot rozprawy

Praca składa się z 7 rozbudowanych rozdziałów. W każdy z nich Autorka omawia inny aspekt prowadzonych przez siebie badań. I tak,

- **Rozdział 1** stanowi ogólne wprowadzenie do zagadnienia ataków algebraicznych, gdzie Autorka omawia ich ideę oraz przedstawia główne narzędzia wykorzystywane do ich realizacji.

- **Rozdział 2** poświęcony jest obliczeniom kwantowym oraz komputerowi kwantowemu firmy D-Wave Inc. Pierwsza część tego rozdziału to ogólne wprowadzenie do obliczeń kwantowych, z uwzględnieniem modelu adiabatycznego wyżarzania kwantowego. Druga część stanowi charakterystykę komputera kwantowego firmy D-Wave, gdzie Autorka przedstawia sposób implementacji oraz realizacji procesu wyżarzania kwantowego na procesorze wyżarzającym, jak również szczegółowo omawia proces rozwiązywania zagadnień optymalizacyjnych (QUBO / Ising), za pomocą procesora D-Wave.

- **Rozdział 3** jest podstawą recenzowanej rozprawy doktorskiej. W szczegółowy sposób Autorka omawia w nim proponowany model transformacji układu równań wielomianowych, opisujących dowolny szyfr blokowy, do problemu optymalizacyjnego w postaci QUBO. Autorka omawia poszczególne kroki transformacji wraz z zastosowanymi metodami ich realizacji. Rozdział zawiera również opis wymagań, jakie powinien spełniać układ, opisujący szyfr blokowy, w celu otrzymania problemu w postaci QUBO o jak najmniejszym rozmiarze.

- **Rozdział 4** przedstawia analizę struktury standardu AES – szyfru blokowego typu SPN, w kontekście przedstawienia go za pomocą układu równań, który przetransformowany do problemu QUBO o możliwie najmniejszej liczbie zmiennych. Autorka duży nacisk postawiła na znalezienie układu efektywnego dla skrzynki podstawieniowej.

- **Rozdział 5** zawiera analizę przedstawienia szyfru blokowego typu ARX, którym jest szyfr Speck, za pomocą takiego układu równań, dla którego otrzyma się jak najmniejszy problem QUBO. Podczas analizy Autorka zwróciła uwagę na zakres rundy oraz na strukturę algebraiczną, nad którą przedstawiono równania, opisujące działanie szyfru Speck.

- **Rozdział 6** opisuje poszukiwania układu równań, opisującego szyfr blokowy o strukturze Feistela, umożliwiającego otrzymanie jak najmniejszego problemu QUBO. Jako przykładowy szyfr wybrano szyfr Simon.

- **Rozdział 7** podsumowuje rozprawę.

  Głównym celem niniejszej rozprawy było opracowanie ataku, polegającego na przekształceniu układu równań wielomianowych, opisującego szyfr blokowy, do problemu optymalizacyjnego w formie QUBO (*ang.* Quadratic Unconstrained Binary Optimization). Problem ten jest równoważny z problemem minimalizacji energii w modelu Isinga, który to z kolei może zostać (co do zasady) rozwiązany na komputerze kwantowym D-Wave. W proponowanym ataku Autorka wykorzystała ideę ataków algebraicznych, jednak zamiast konstruować układy nad-określone, skupiła się na znalezieniu układu dającego możliwie jak najmniejszy docelowy problem QUBO.

Autorka wzięła przy tym, przede wszystkim, pod uwagę problem osadzania problemu (*ang.* embedding) w fizycznej strukturze obliczeniowej procesora wyżarzającego, podczas którego skalowane są wartości macierzy połączeń, reprezentującej rozwiązywany problem optymalizacyjny oraz tworzone są łańcuchy fizycznych kubitów (reprezentujące logiczne zmienne optymalizacyjne). Konieczność zastosowania procedury osadzania wynika z ograniczeń obecnych komputerów wyżarzających (np. brak kubitów lub połączeń między nimi).

Doktorantka umiejętnie dostosowała model transformacji układu równań wielomianowych o wielu zmiennych, opisujący dowolny szyfr blokowy, do problemu QUBO / Isinga. Chociaż poszczególne kroki modelu transformacji były znane już wcześniej, w prezentowanym podejściu Autorka dobrała takie metody, które zapewniają, że globalne rozwiązanie problemu optymalizacyjnego QUBO jest rozwiązaniem układu opisującego szyfr oraz w jak najmniejszym stopniu zwiększają rozmiar docelowego problemu optymalizacyjnego. Pokazano, że proponowana metoda transformacji umożliwia jednoznaczne odzyskanie klucza głównego.

Wynika z tego, że jednoznacznie wyznaczenie klucza wymaga wyznaczenia stanu podstawowego w modelu Isinga. Wyniki eksperymentów dla obecnych kwantowych wyżarzaczy D-Wave pokazując, że prawdopodobieństwo znalezienia stanu podstawowego maleje wykładniczo wraz ze rozmiaru układu, np. Quantum Inf. Process. **21**, *141 (2022). Co oznacza, że dla dostatecznie dużej ilości zmiennych (w praktyce już nawet kilkudziesięciu) wykonanie opracowanego w ramach rozprawy algorytmu na komputerach D-Wave zasadniczo nie przyniesie oczekiwanego rezultatu.*

Może właśnie z tego powodu Autorka nie zdecydowała się umieścić wyników eksperymentów przeprowadzonych z wykorzystaniem procesora D-Wave dla wyznaczonych przez siebie instancji QUBO. Wydaje mi się, że byłby to wartościowy element pracy, który z drugiej strony pomógłby rzucić nieco inne światło na zagadnienie testowania i walidacji technologi kwantowej w omawianym kontekście.

Oczywiście inna kwestią jest rozpatrywanie otrzymanych wyników z punktu widzenia ich wyżarzenia na "idealnym" kwantowym procesorze. Wówczas, jak zauważa sama Autorka, interesującym staje się zbadania złożoności obliczeniowej dla rozpatrywanych klas problemów. Gdyby złożoność ta skalowała się jak $O(\exp(\alpha N^{\beta}))$ (a istnieją powody aby przypuszczać, że tak może istotnie być) to wówczas można by zbadać czy opisany algorytm może być lepszy niż najlepszy atak klasyczny dla rozważanego problemu. W szczególności dla $\alpha = 1$ i $\beta = 1/2$ najlepszy rezultat ataku algebraicznego wykorzystującego wyżarzanie kwantowe pozwoliłoby osiągnąć dla szyfru Speck128/256, dla którego atak ten może być skuteczny na 32 z 34 (tj. 94% liczby rund całego szyfru) rund, co jest w istocie lepszym wynikiem niż najlepszy atak klasyczny, gdzie przy użyciu kryptoanalizy różnicowej można złamać 25 z 34 (tj. 74% liczby rund całego szyfru) rund szybciej niż przez wyczerpujące przeszukanie. Uważam, iż jest to bardzo interesujący problem sam w sobie.

Równie interesujące są tutaj dwa inne aspekty, które wychodzą znacznie poza rozprawę doktorską, ale mogą potencjalnie wyznaczyć nowe kierunki badań. Są one blisko związane z tematyką prezentowaną w rozprawie, a mianowicie:

1. zbadanie możliwość opracowania algorytmu, w którym rozwiązanie zakodowanie jest w stanach wzbudzonych nieskoenergetycznych (podobnie można by się zastanowić czy

nie jest możliwe opracowanie skutecznego ataku, który korzysta z próbkowania z danej dystrybucji – która można realizować na komputerze wyżarzającym – zamiast polegać wyznaczaniu stanu podstawowego),

2. zbadanie jakie są ograniczenia klasycznych algorytmów inspirowanych fizycznie (lecz niekoniecznie kwantowych) na możliwość rozwiązywania instancji QUBO / Isinga dla dyskutowanych w pracy problemów kryptograficznych. Dobrym przykładem może tu być algorytm symulowanej bifurkacji, np. H. Goto, at al., Science Advances **7**, 6 (2022). Algorytm ten koduje rozwiązanie problemu QUBO / Isinga w stanie stacjonarnym procesu dynamicznego, który jest następnie wyżarzany. Taka metoda pozbawione jest tych wad, które Autorka napotkała przy próbie wykonania algorytmu na komputerach firmy D-Wave. Przykładowo nie jest konieczne osadzanie problemów optymalizacyjnych, jako że opisany algorytm radzi sobie nawet z gęstymi topologiami typu *all-to-all*.

3 Uwagi techniczne *nie* wpływające na część merytoryczną

Pracę napisane jest starannie i rzetelnie, bardzo dobrze się ją czyta.

Nie zmienia to jednak faktu, że mogłaby być on znacznie krótsza. Ponad 200 stron to jednak dużo. Rozwlekłość należy traktować jako negatywną cechę wypowiedzi pisemnej. I tak, bardzo dużo uwagi poświęcono kwestiom znanym i dobrze zbadanym np. podstawom obliczeń kwantowych, w szczególności kwantowemu wyżarzaniu (włączając w to jego aspekty fizyczne). W moim odczuciu taki zabieg jest zupełnie zbyteczny gdyż Autorka i tak nie dyskutuje w pracy żadnych eksperymentów na komputerach kwantowych, a skupia się wyłącznie na analizie matematycznej swoich badań. Uważam, iż z łatwością można było zaoszczędzić przynajmniej 1/3 wszystkich stron.

Trudno mi również zrozumieć dlaczego Autorka zdecydowała się napisać dysertację w języku polskim. Taki stan rzeczy znacznie ogranicza grono potencjalnych odbiorców. Nauka ma jednak charakter międzynarodowy. Jest to o tyle dziwne, iż dwa artykuły naukowe na których praca została oparta zostały opublikowane w języku angielskim.

Jakość większości rysunków mogłaby być znacznie lepsza (np. Rysunek 57 jest słabo czytelny, źle wyskalowany i nie mam w ogóle podpisanych osi). Uważam, że można to było zrobić stosunkowo niewielkim nakładem pracy. Przyczyniłoby się to do zwiększenia jakości pracy i ogólnie lepszego jej odbioru.

Należy jednak podkreślić, iż powyższe uwagi są natury technicznej i w żaden sposób nie *wpływające na ocenę merytoryczną rozprawy.*

4 Ocena końcowa i wnioski

Rozprawa doktorska Pani kpt. mgr inż. Elżbiety BUREK traktuje o wykorzystaniu kwantowych komputerów wyżarzających D-Wave do przeprowadzenia ataku na szyfry blokowe. W przeciwieństwie do klasycznych komputerów, kwantowe procesory wyżarzające wymagają specjalnego sposobu programowania i nie każde zagadnienie można na nich rozwiązać. W celu wykonania algorytmu na komputerze D-Wave należy najpierw opracować odpowiadający mu problem QUBO (lub równoważnie modelu Isinga). Nie jest to prosty problem, a jego rozwiązanie wymaga

pomysłowości. W mojej ocenie doktorantka rozwiązała postawione problemy badawcze i użyła do tego celu właściwych metod badawczych. Oryginalnym osiągnięciem Autorki są:

*W*1 Zdefiniowanie układu jednoznacznie wyznaczającego skrzynkę podstawieniową oraz zaproponowanie metody poszukiwania dla niej układu efektywnego, w kontekście dalszych przekształceń do problemu QUBO.

*W*2 Określenie zakresu wartości wagi kary przy linearyzacji dla zastosowanej metody transformacji układu równań do problemu optymalizacyjnego w postaci QUBO i zastosowanego procesora D-Wave do rozwiązania tego problemu. Pokazanie, że problem linearyzacji układów równań opisujących przeanalizowane szyfry blokowe nie jest problemem NP-trudnym.

*W*3 Zdefiniowanie wymagań dla układów równań opisujących szyfry blokowe oraz pokazanie sposobu konstruowania układów równań wielomianowych o wielu zmiennych opisujących szyfry blokowe o najpopularniejszych typach struktur tak, aby docelowy problem w postaci QUBO był możliwie najmniejszy.

*W*4 Uzyskanie rozmiarów QUBO dla standardu AES znacznie mniejszych niż opublikowanych do tej pory oraz istotnie mniejszych niż dla problemów kryptografii asymetrycznej.

Uważam, że przedstawiona mi do oceny rozprawa doktorska spełnia wymogi ustawowe stawiane pracom doktorskim w dziedzinie nauk inżynieryjno-technicznych, dyscyplinie informatyka techniczna i telekomunikacja. Wnoszę zatem o jej przyjecie przez Radę Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego oraz o dopuszczenie Pani kpt. mgr inż. *Elżbiety BUREK* do dalszych etapów przewodu doktorskiego.

dr hab. Bartłomiej Gardas

Bartłomiej Gardas

Podpisany certyfikatem kwalifikowanym przez
Bartłomiej Gardas
2023-05-10 22:05:09+0200
Podpisany z użyciem eDO App.