Warszawa, 20 maja 2023r.

dr hab. Mirosław Kurkowski, prof. UKSW, prof. WSPol

- **Instytut Informatyki**
  Uniwersytet kard. St. Wyszyńskiego w Warszawie
- **Instytut Służby Kryminalnej**
  Wyższa Szkoła Policji w Szczytnie

Recenzja rozprawy doktorskiej kpt. mgr inż. Elżbiety Burek

Ataki algebraiczne na szyfry blokowe z wykorzystaniem wyżarzania kwantowego

Promotor: dr hab. Marek Kojdecki, prof. WAT

Promotor pomocniczy: dr inż. Michał Wroński

Niniejsza recenzja została sporządzona na prośbę Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej wyrażonej w odpowiednim piśmie. Opiniowana rozprawa omawia prace badawcze dotyczące opracowania ataków kryptoanalitycznych z wykorzystaniem technik kwantowych. Ataki te wykorzystują przekształcenie rozwiązania układu równań wielomianowych określających badany szyfr do problemu optymalizacyjnego QUBO (binarnego zadania najmniejszych kwadratów bez ograniczeń).

Wprowadzenie

Dzisiejsza kryptografia oferuje wiele algorytmów i technik służących do zabezpieczania danych w sieciach oraz innych systemach komputerowych. Już od lat siedemdziesiątych XX wieku, zarówno rozwiązania symetryczne, jak i asymetryczne, w tym algorytmy klucza publicznego, zapewniają wiele celów związanych z bezpieczeństwem informacji. Jednym z najpopularniejszych algorytmów stosowanych w praktyce jest algorytm RSA opracowany przez Rivesta, Shamira i Adlemana, który bazuje na problemie faktoryzacji, czyli rozkładzie dużych liczb na czynniki. Udowodniono, że problem ten jest trudny obliczeniowo i obecnie nie są znane metody skutecznego rozwiązywania go dla praktycznie stosowanych rozmiarów liczb.

Kryptolodzy od dawna z uwagą obserwują postęp w dziedzinie technik kwantowych oraz budowy komputerów kwantowych, które mogą być bardziej efektywne w obliczeniach niż komputery tradycyjne. Algorytm Petera Shora, opublikowany w 1994 roku, umożliwia szybkie rozkładanie liczb złożonych na czynniki pierwsze, ale wymaga użycia komputera kwantowego z tysiącami lub setkami tysięcy kubitów. Choć takie komputery jeszcze nie

istnieją, postęp w ich budowie jest zagrożeniem dla obecnie stosowanej kryptografii, gdyż komputery kwantowe mogą złamać wiele kryptosystemów, których bezpieczeństwo opiera się na trudności rozwiązywania pewnych problemów obliczeniowych.

Nie jest pewne, czy dalszy rozwój komputerów kwantowych może stanowić realne zagrożenie dla algorytmów kryptograficznych takich jak RSA, ale ze względu na możliwe ryzyko, podjęto już badania mające na celu opracowanie bezpiecznych konstrukcji odpornych na ewentualne ataki ze strony komputerów kwantowych. Obliczenia kwantowe mogą być stosowane w kryptoanalizie także w celach innych niż faktoryzacja. Prezentowana rozprawa doktorska opisuje właśnie takie zastosowania. Badania w tym zakresie są w pełni uzasadnione i ważne z puntu widzenia zabezpieczeń komunikacji i przechowywania danych w sieciach i systemach komputerowych.

Zawartość rozprawy

Recenzowana rozprawa liczy 207 stron razem ze Spisem Treści oraz Bibliografią. Moim zdaniem układ rozprawy budzi pewne zastrzeżenia. W moim odczuciu zbyt dużo miejsca zostało poświęcone przedstawieniu zagadnień związanych z obliczeniami kwantowym i budową komputera D-Wave. Zacytowana w pracy literatura przedmiotu liczy 66 pozycji. Mam wrażenie, że mogłaby być ona (nieco) większa. Można by zacytować na przykład więcej prac dotyczących SAT-kryptoanalizy.

We Wprowadzeniu autorka przedstawiła cel naukowy rozprawy: *Celem postawionym w niniejszej rozprawie jest dostosowanie modelu transformacji układu równań do postaci problemu optymalizacyjnego, rozwiązywanego za pomocą wyżarzania kwantowego, do wykorzystania w atakach algebraicznych na szyfry blokowe, osiągając rozmiary problemów mniejsze, niż dotychczas opublikowano.*

Do osiągnięcia postawionego celu mgr inż. Burek proponuje realizację następujących zadań:

- *Przeanalizowanie implementacji procesu wyżarzania kwantowego w komputerze firmy D-Wave.*
- *Dostosowanie modelu transformacji układu równań wielomianowych do problemu optymalizacyjnego w postaci QUBO, w celu wykorzystania go w atakach algebraicznych na szyfry blokowe przy użyciu komputera firmy D-Wave oraz scharakteryzowanie efektywnego układu równań wielomianowych, umożliwiającego uzyskanie możliwie najmniejszego problemu QUBO.*
- *Przeanalizowanie struktury wybranych szyfrów blokowych, w celu znalezienia układu efektywnego.*

– *Dla małych instancji analizowanych szyfrów, przeprowadzenie proponowanego ataku na dostępnych zasobach komputera D-Wave.*

W skład rozprawy poza Wprowadzeniem wchodzi siedem rozdziałów.

W pierwszym rozdziale recenzowanej pracy doktorskiej mgr inż. Burek przedstawiła ogólne wprowadzenie do ataków algebraicznych. Została omówiona idea tych ataków oraz przedstawione główne narzędzia wykorzystywane do ich realizacji. W szczególności, autorka skupiła się na omówieniu algorytmów baz Gröbnera (wraz z algorytmem Buchbergera, F_4 i F_5), metody linearyzacji, algorytmu XL (wraz z odmianami FXL i XSL), algorytmu ElimLin oraz technik zastosowania do tych celów SAT-solwerów.

Rozdział drugi skupia się na obliczeniach kwantowych i omawia szczegółowo komputer kwantowy D-Wave. Pierwsza część rozdziału wprowadza do ogólnych zasad obliczeń kwantowych, ze szczególnym uwzględnieniem modelu adiabatycznych obliczeń kwantowych oraz wyżarzania kwantowego. Druga część skupia się na charakterystyce komputera D-Wave, przedstawiając sposób jego implementacji oraz sam proces wyżarzania kwantowego. Ponadto, szczegółowo opisany został proces rozwiązywania problemów optymalizacyjnych za pomocą tego komputera.

Rozdział trzeci to kluczowy element rozprawy doktorskiej, w którym przedstawiony jest proponowany model translacji problemu rozwiązania układu równań wielomianowych opisujących szyfr blokowy na problem optymalizacyjny w postaci QUBO. W rozdziale szczegółowo omówiono kolejne kroki translacji i przedstawiono wykorzystane metody ich realizacji. Zakończenie rozdziału stanowi opis wymagań, które powinien spełniać układ opisujący szyfr blokowy, aby uzyskać problem w postaci QUBO o możliwie najmniejszym rozmiarze co jest istotne z punktu widzenia efektywności obliczeń.

W rozdziale czwartym autorka przedstawia analizę struktury standardu AES - szyfru blokowego typu SPN - w celu przedstawienia go za pomocą układu równań, który przetransformowany do problemu QUBO da jak najmniejszy rozmiar problemu optymalizacyjnego. W szczególności, poświęcono wiele uwagi na znalezienie efektywnego układu dla skrzynki podstawieniowej.

Rozdział piąty opisuje analizę szyfru blokowego typu ARX, tj. szyfru Speck, w celu przedstawienia go za pomocą układu równań, który po przetransformowaniu do problemu QUBO da jak najmniejszy rozmiar problemu optymalizacyjnego. W trakcie analizy skupiono się na zakresie rundy oraz na strukturze algebraicznej, nad którą przedstawiono równania, opisujące działanie szyfru.

W rozdziale szóstym przedstawiono poszukiwania układu równań, który opisuje szyfr blokowy o strukturze Feistela, a który umożliwiłby otrzymanie jak najmniejszego problemu QUBO. Jako przykład szyfru blokowego wybrano szyfr Simon.

Rozdział siódmy zawiera podsumowanie recenzowanej rozprawy.

Podsumowując szczegółowo wyniki zawarte w rozprawie należy podkreślić, że:

Przedstawiane w rozprawie prace są związane bezpośrednio z bieżącym i ważnym trendem współczesnej kryptografii stosowanej. Wychodzą również naprzeciw procesowi standaryzacyjnemu rozpoczętemu przez amerykański Narodowy Instytut Standardów NIST. Celem rozprawy było opracowanie nowego sposobu ataku na szyfry blokowe, który polegałby na translacji problemu rozwiązania układu równań wielomianowych opisującego szyfr do problemu optymalizacyjnego w postaci QUBO. Zamiast konstruować układy nadokreślone, autorka skupiła się na znalezieniu układu dającego najmniejszy możliwy problem QUBO. W tym celu przeanalizowano proces wyżarzania kwantowego oraz implementację komputera kwantowego D-Wave, który umożliwia rozwiązywanie problemów optymalizacyjnych. Ostatecznie, proponowana metoda ataku wykorzystuje ideę ataków algebraicznych, jednak z nowym podejściem polegającym na transformacji układu równań do problemu QUBO.

Prace badawcze przeprowadzone przez autorkę składały się z kilku etapów. Ich wynikiem było zdefiniowanie efektywnego układu równań opisującego szyfr blokowy, umożliwiającego uzyskanie jak najmniejszego problemu optymalizacyjnego. Głównym zadaniem badawczym było znalezienie efektywnego układu równań dla trzech najpowszechniejszych struktur szyfrów blokowych: SPN (AES), ARX (Speck) i Feistela (Simon).

W wyniku przeprowadzonych rozważań i eksperymentów opracowano efektywny układ równań opisujących szyfr blokowy oraz zaproponowano metodę poszukiwania efektywnego układu równań dla skrzynki podstawieniowej w celu dalszych przekształceń do problemu optymalizacyjnego w postaci QUBO. Zdefiniowano wymagania dla układów równań opisujących szyfry blokowe oraz zaprezentowano sposób konstruowania układów równań wielomianowych o wielu zmiennych opisujących szyfry blokowe o najpopularniejszych typach struktur, w celu uzyskania jak najmniejszego docelowego problemu w postaci QUBO. Uzyskano także rozmiary problemów QUBO dla standardu AES znacznie mniejsze niż dotychczas opublikowane.

Podsumowując tę część recenzji stwierdzam jednoznacznie, że moim zdaniem mgr inż. Elżbieta Burek odpowiedziała na postawione pytania i zrealizowała postawione sobie Cele badawcze.

Uwagi polemiczne i krytyczne oraz elementy dyskusyjne

Przedstawione niżej uwagi nie zmniejszają moim zdaniem wartości naukowej rozprawy i nie mają wpływu na pozytywną opinię pracy jako całości. Zamieszczone uwagi mogą też stanowić pole do dalszych badań.

1. W moim odczuciu w pierwszych częściach rozprawy należałoby zadbać o większą precyzję wypowiedzi. Sformułowania typu: „przyspieszenie kwantowe", „problemy trudne lub niewykonalne", „problemy gęste i rzadkie", „nie wszystkie przypadki problemów NP-trudnych są NP-trudne" i inne wymagałyby moim zdaniem przeformułowania lub dookreślenia.
2. W pracy zdarzają się pojęcia nieokreślone lub niezdefiniowane. Na przykład o jakich pierścieniach mowa na stronie 14? O jakim ideale mowa na stronie 15tej? Co to są S-wielomiany (str. 16)?
3. Czy na pewno: „Obecne narzędzia, wykorzystywane do ataków algebraicznych, nie umożliwiają przeprowadzenia ataku w czasie krótszym, niż atak pełnego przeszukiwania."??
4. Autorka rozprawy przedstawiła dwie metody przekształcenia układu równań wielomianowych na problem optymalizacyjny QUBO: linearyzację i kwadratyzację. Do dalszych badań wybrała linearyzację, jednak w uzasadnieniu swojego wyboru skupiła się jedynie na kwestii wartości współczynnika kary. W celu pełniejszego porównania obu metod, warto by było przeanalizować ich zastosowanie w całym procesie transformacji.
5. W celu realizacji procesu linearyzacji, autorka wykorzystała metodę redukcji Rosenberga. Udowodniła, że dla badanych szyfrów blokowych, ta metoda ma wielomianową złożoność obliczeniową. Niemniej jednak, autorka nie przeanalizowała wykonania procesu linearyzacji przy użyciu innych znanych metod.
6. W celach badawczych autorka wybrała trzy różne szyfry, z których każdy reprezentował inną strukturę algorytmów blokowych. Jednym z przykładów był szyfr Simon, który reprezentował strukturę sieci Feistela, w której operacja nieliniowa realizowana jest za pomocą bitowej operacji AND. Jednak, aby analiza była kompletna, warto byłoby przeanalizować także inny szyfr reprezentujący strukturę sieci Feistela, w którym operacja nieliniowa jest realizowana za pomocą skrzynki podstawieniowej, np. szyfr DES. Możliwe, że ze względu na strukturę szyfru DES, kryptoanaliza z wykorzystaniem wyżarzania kwantowego przyniosłaby lepsze wyniki, niż dla pozostałych, przeanalizowanych w pracy, algorytmów.
7. Autorka do oceny uzyskanych wyników skorzystała z dostępnych heurystycznych oszacowań złożoności obliczeniowej procesu wyżarzania kwantowego. Niemniej jednak, pełna ocena jakości pracy wymaga dokładnego określenia złożoności obliczeniowej tego

procesu. Należy jednak zaznaczyć, że wyznaczenie złożoności obliczeniowej procesu wyżarzania kwantowego jest trudne, zarówno ogólnie, jak i w szczególnych przypadkach, które były analizowane w pracy. W związku z tym, taka analiza może być przedmiotem dalszych badań.

Uwagi redakcyjne

Nie znalazłem błędów w części matematycznej rozprawy. Jak w każdej pracy zdarzają się literówki, błędy redakcyjne i stylistyczne. Kilka przykładów to:

- s. 8, *przeszkujania*,

- s. 14, *przez około pięćdziesięciu lat kryptografia symetryczna ...*,

- s. 16, *Niech będzie dany układ m równań kwadratowych, n zmiennych.*

- s. 20, *...teorię stojącą za komputerem kwantowym*,

- s. 70, *...szyfr blokowy można przedstawić jako równania wielomianowych...*,

Wniosek końcowy

Przedstawione w recenzowanej rozprawie doktorskiej rozważania związane z konstruowaniem metod ataków kryptoanalitycznych z wykorzystaniem technik kwantowych dotyczą ważnych i bieżących problemów kryptografii. Rozprawa doktorska kpt. mgr inż. Elżbiety Burek zawiera wiele oryginalnych oraz interesujących wyników. Moje uwagi krytyczne oraz polemiczne zawarte w recenzji nie zmniejszają mojej pozytywnej opinii o rozprawie jako całości.

Biorąc pod uwagę wyniki naukowe przedstawione w recenzowanej rozprawie doktorskiej kpt. mgr inż. Elżbiety Burek stwierdzam, że moim zdaniem, praca ta spełnia wymagania stawiane rozprawom doktorskim przez obowiązującą aktualnie w Polsce Ustawę o Stopniach i Tytule Naukowym. Stawiam zatem wniosek o dopuszczenie kpt. mgr inż. Elżbiety Burek do dalszych etapów przewodu doktorskiego prowadzonego w dziedzinie nauk inżynieryjno-technicznych w dyscyplinie Informatyka techniczna i telekomunikacja przez odpowiednią Radę Dyscypliny Naukowej Wojskowej Akademii Technicznej.