Warszawa, 12 maja 2021r.

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

- **Instytut Informatyki**
  Uniwersytet kard. St. Wyszyńskiego w Warszawie
- **Zakład Cyberbezpieczeństwa**
  Wyższa Szkoła Policji w Szczytnie

Recenzja rozprawy doktorskiej mgra inż. Michała Andrzejczaka

Acceleration of lattice based algorithms

Promotor: dr hab. inż. Andrzej Paszkiewicz, prof. WAT

Niniejsza recenzja została sporządzona na prośbę Rady Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej wyrażonej w odpowiednim piśmie przez prof. WAT, dra hab. inż. Zbigniewa Tarapatę (pismo nr WYCH/N/00112/2021) oraz uchwałach: 14/RDN ITiT/2021 i 15/RDN ITiT/2021. Opiniowana rozprawa dotyczy prac badawczych związanych z opracowaniem nowych algorytmów i technik kryptograficznych odpornych na możliwe, przewidywane, przyszłe ataki wykorzystujące komputery kwantowe i algorytmy wymagające ich stosowania (tzw. Post Quantum Cryptography). Przewód doktorski prowadzony jest zgodnie z tzw. „starą procedurą" w dziedzinie nauk technicznych, w dyscyplinie naukowej Informatyka.

Wprowadzenie

Kryptografia daje dzisiaj wiele algorytmów i technik mających zastosowanie w systemach zabezpieczeń danych w sieciach i innych systemach komputerowych. Od lat siedemdziesiątych ubiegłego wieku rozwiązania najpierw symetryczne, a potem, po opracowaniu kryptografii asymetrycznej, również klucza publicznego, gwarantują zapewnienie wielu celów związanych z bezpieczeństwem informacji. Jednym ze sztandarowych algorytmów stosowanych w praktyce jest słynny algorytm RSA Rivesta, Shamira i Adlemana bazujący na problemie faktoryzacji, czyli rozkładzie na czynniki dużych liczb naturalnych. Udowodniono, że problem ten jest trudnym obliczeniowo, to jest nie są obecnie znane metody mogące efektywnie rozwiązywać takie zagadnienia w zakresie stosowanych w praktyce rozmiarów liczb.

Od wielu lat kryptolodzy patrzą z niepokojem na rozwój technik kwantowych, a zwłaszcza na prace związane z budową komputerów kwantowych, urządzeń wykorzystujących inne, bardziej efektywne niż tradycyjne metody obliczeń. Opublikowany

przez Petera Shora w 1994 roku algorytm pozwala na szybki rozkład na czynniki pierwsze liczb złożonych. Algorytm ten ma złożoność czasową $O((\log n)^3)$ i pamięciową $O(\log n)$, jednak jego wykorzystanie praktyczne wymaga zastosowania komputera kwantowego o dużej, w tysiącach lub nawet setkach tysięcy liczonej liczbie tzw. kubitów. Jak na razie takie komputery nie istnieją, jednak bieżący postęp w dziedzinie konstrukcji takich urządzeń jest stale rosnącym zagrożeniem dla aktualnie stosowanej kryptografii.

Nie wiadomo, czy powstanie efektywny komputer kwantowy mogący zagrozić w praktyce algorytmowi RSA i innym tego typu rozwiązaniom, jednak ze zrozumiałych względów zostały już rozpoczęte prace badawcze nad opracowaniem bezpiecznych konstrukcji odpornych na ewentualne ataki dokonane przez komputery kwantowe.

Recenzowana rozprawa doktorska doskonale wpisuje się w tę tematykę. Przedstawione w niej nowe, autorskie rozwiązania dotyczą zarówno sfery algorytmicznej jak i sprzętowej tzw. kryptografii postkwantowej. Zajmowanie się tą stosunkowo nową i ważną gałęzią kryptografii jest jak najbardziej uzasadnione i bardzo ważne.

Zawartość rozprawy

Recenzowana rozprawa liczy 81 stron, nie licząc Spisu Treści, dodatków oraz Bibliografii. W mojej opinii układ rozprawy budzi pewne zastrzeżenia. Nie rozumiem dlaczego autor zdecydował się na wyodrębnienie jak rozdziały jedno-dwustronnych rozdziałów 2 oraz 7. Treści tam zawarte mogłyby zostać dodane jako wprowadzenia w kolejnych rozdziałach. Również rozdział 11ty, zawierający syntetyczne podsumowanie opisywanych w rozprawie wyników badań powinien mieć moim zdaniem inny status. Jednak zaznaczyć należy, że kolejność opisywanych treści jest odpowiednia. Zacytowana w pracy literatura przedmiotu liczy 115 pozycji i biorąc pod uwagę prowadzone w rozprawie rozważania jest moim zdaniem dobrana adekwatnie.

W rozdziale trzecim autor przedstawił podstawowe problemy/pytania badawcze na jakie będzie się starał odpowiedzieć w swoich rozważaniach.

Są to:

Pytanie I: Czy redukcję sieci kratowej można przyspieszyć za pomocą specjalistycznego sprzętu?

Jest to podstawowy problem jaki rozwiązuje doktorant w pierwszej części tej pracy. Redukcja wektorów kratowych jest operacją podstawową w każdym algorytmie przesiewania kratowego i jest to najczęściej stosowana operacja w tego typu algorytmie.

Pytanie II: Czy ewentualny nowy akcelerator może znaleźć zastosowanie w praktyce?

Wyniki teoretyczne często odbiegają od możliwości ich praktycznego zastosowania. W wielu przypadkach obciążenie komunikacyjne między procesorem a FPGA lub pojemność pamięci układów FPGA może prowadzić do braku możliwości zastosowania algorytmu w praktyce.

Pytanie III: Czy i jak można oszacować w rozpatrywanych przypadkach granicę współczynnika przyspieszenia dla nowoczesnych układów FPGA?

Jak każde rozwiązania sprzętowe także nowoczesne układy FPGA mają swoje ograniczenia techniczne. Dodanie dodatkowych akceleratorów może nie zawsze dać pozytywny wynik.

Pytanie IV: W jaki sposób przyspieszenie wpływa na obliczenia prowadzone dla rozwiązań rozpatrywanych problemów?

Oszacowanie może obejmować maksymalny wymiar sieci i koszt rozwiązywania instancji SVP.

W kolejnych rozdziałach swojej rozprawy doktorskiej mgr Andrzejczak opisuje autorskie badania pozwalające odpowiedzieć na powyższe pytania.

W skład rozprawy poza Wstępem wchodzi jedenaście rozdziałów.

W rozdziale pierwszym rozprawy mgr Andrzejczak prezentuje podstawowe pojęcia matematyczne wykorzystywane w dalszych częściach dysertacji. Ustanawiają one odpowiedni kontekst matematyczny dla wprowadzania opisywanych dalej i realizowanych sprzętowo operacji. I tak, kolejno, na bazie wielu ważnych i uznanych pozycji literaturowych, doktorant przytacza znane, podstawowe definicje teorii krat (algebry liniowej) oraz sformułowania problemów najkrótszego (SVP – Shortest Vector Problem) i najbliższego wektora w kracie (CVP – Closest Vector Problem). Przedstawiono także estymację wartości rozwiązania tych problemów dla danej, wybranej kraty. Rozdział ten kończą definicje problemów LWE oraz LWR wraz z opisem odpowiedniego kontekstu.

Kolejne rozdziały rozprawy można w zasadzie podzielić na dwie części. Pierwsza z nich, zawierająca rozdziały 2 - 6 dotyczy rozwiązań akceleracji sprzętowej metod rozwiązywania problemu najkrótszego wektora w kracie (SVP – Shortest Vector Problem). Druga część składająca się z rozdziałów 7 - 11 przedstawia autorskie wyniki uzyskane przez mgra Andrzejczaka w zakresie efektywnych implementacji postkwantowych algorytmów klucza publicznego.

Rozdział drugi pracy zawiera streszczenie ww. pierwszej części rozprawy. Autor przedstawia tutaj schemat powiązań pomiędzy kolejnymi rozdziałami oraz nakreśla poruszane w swoich badaniach najważniejsze problemy.

W rozdziale trzecim doktorant zawarł wprowadzenie do metod rozwiązywania problemu najkrótszego wektora w kracie (SVP). W szczególności opisano metodę zwaną przesiewaniem kraty, która jest obiektem dalszych badań. Zgodnie z obecnym stanem wiedzy właśnie ta metoda jest obecnie najpowszechniej stosowana w praktyce do rozwiązywania problemu SVP. Mgr Andrzejczak na podstawie odpowiednio dobranej literatury przedstawia historię rozwoju badań nad konstruowaniem algorytmów rozwiązujących problem SVP oraz omawia szczegółowo główne założenia wybranych przykładów algorytmów i metod przyspieszania procesu przesiewania. Kolejno, w ramach przeglądu literatury, omówiono dotychczas opublikowane prace z zakresu implementacji i akceleracji algorytmu przesiewania Gaussa, wybranego przez doktoranta do dalszych badań. Ponieważ w literaturze brak jest prac na temat algorytmów przesiewania realizowanych w układach programowalnych autor przytacza i opisuje pracę dotyczącą rozwiązywania problemu SVP za pomocą metody enumeracji kraty wykorzystującej układy programowalne FPGA. Rozdział ten kończy się postawieniem czterech, zaprezentowanych wcześniej, pytań badawczych, które będą przedmiotem rozważań pierwszej części rozprawy.

W rozdziale czwartym przedstawiono autorską metodę bazowej operacji wykorzystywanej w algorytmach przesiewania kraty jaką jest skracanie wektorów w układzie programowalnym. Doktorant proponuje tutaj odpowiednio zaprojektowany układ logiczny, który jest zoptymalizowany wydajnościowo dla kolejnych operacji matematycznych. Podana jest również analiza efektywności układu i zależności czasowych związanych z prowadzonymi obliczeniami. Ciekawym rezultatem prowadzonych prac badawczych jest zaproponowana w celu osiągnięcia optymalnych rezultatów metoda polegająca na zastąpieniu operacji dzielenia przez sekwencję prostych instrukcji warunkowych, dobranych odpowiednio do rozwiązywanych zagadnień. Układy realizujące operacje podstawowe są następnie odpowiednio łączone i ich działanie jest uzupełniane dodatkowymi rejestrami przesuwnymi. Ma to na celu osiągnięcie możliwości potokowej realizacji prowadzonych obliczeń, a tym samym zwiększenie wydajności układu. Na koniec czwartego rozdziału mgr Andrzejczak analizuje przydatność opracowanej konstrukcji dla różnych typów i rozmiarów kraty.

W rozdziale piątym przedstawiono analizę wydajności opracowanego akceleratora w rzeczywistym środowisku uwzględniając koszty transferu danych w przypadku trzech różnych scenariuszy. Zbadano najpierw wydajność przesiewania na standardowych procesorach oraz wyprowadzono zależności opisujące czas transferu pojedynczego punktu na kracie. Kolejno dane te zostały wykorzystane do analizy wydajności akceleratora w trzech przypadkach, w których wstępująco każdy kolejny jest bardziej zaawansowany od poprzedniego i oferuje większe przyspieszenie względem implementacji programowej. Autor

zaproponował tutaj między innymi zastosowanie dodatkowych elementów logicznych uzupełniających działanie opracowanego wcześniej akceleratora. Rozdział kończy się komentarzem autora co do odniesienia opracowanych technik do innych algorytmów.

Rozdział szósty przedstawia nowe, autorskie wyniki kompilacji dla opracowanego rozwiązania. Sformułowany i rozwiązany został problem optymalizacyjny polegający na maksymalizacji osiągniętego przyspieszenia. Następnie dokonano analizy porównawczej kosztów opracowanego rozwiązania i potencjalnych oszczędności w porównaniu do standardowych implementacji. Oszacowanie zostało wykonane dla dwóch wybranych urządzeń oraz przy wykorzystaniu dwóch instancji dostępnych w chmurze Amazon. Podjęto także próbę odpowiedzi na pytania jak uzyskane przyspieszenie może wpłynąć na rozmiar aktualnie rozwiązywanego problemu SPV oraz jak blisko ideału plasują się osiągnięte rezultaty. W ostatniej części rozdziału zawarto podsumowanie osiągniętych rezultatów opisanych w części pierwszej rozprawy.

W rozdziale siódmym doktorant czyni wstęp do drugiej części rozprawy. Zawarto tutaj krótkie wprowadzenie do prezentowanych dalej treści związanych ze sprzętową realizacją postkwantowego algorytmu Round5. Rozdział ten kończy się przeglądem literatury w dziedzinie sprzętowych implementacji kryptografii postkwantowej.

Rozdział ósmy poświęcony jest algorytmowi Round5. Przedstawiono tutaj jego elementy składowe. Rozdział zawiera także wprowadzenie potrzebne do zrozumienia dalszych części pracy. Autor bazuje tutaj na dokumentach zgłoszonych do organizowanego przez NIST konkursu na nowy standard postkwantowy.

W rozdziale dziewiątym mgr Andrzejczak przedstawia wyniki autorskich badań dotyczących wysokowydajnej implementacji sprzętowej algorytmu Round5. Przedstawiono tutaj implementację algorytmu w modelu „software/hardware codesign”, w którym tylko najbardziej czasochłonne operacje są realizowane sprzętowo, natomiast pozostałe wykonywane są programowo na procesorze ARM. W kolejnych częściach rozdziału przedstawiono schemat układu realizującego fragmenty Round5. Istotnym elementem zaproponowanym tutaj przez autora jest wykorzystywany w Round5 moduł odpowiedzialny za mnożenie wielomianów. W kolejnym kroku autor prezentuje rozszerzenie zaprezentowanego wcześniej schematu o pozostałe brakujące elementy całego algorytmu. Dzięki temu uzyskano w pełni sprzętową implementację wybranego algorytmu.

W przedostatnim rozdziale autor zawarł opis próby realizacji sprzętowej tego samego algorytmu, jednak z innym kryterium optymalizacyjnym – minimalizacją zajętości logicznej. W tym celu zaproponowano modyfikację do opracowanego wcześniej modułu mnożącego wielomiany tak, aby była możliwość jego skalowania. Te i kilka innych zmian pozwoliły

uzyskać kompaktowy rozmiar algorytmu, porównywalny do niektórych blokowych algorytmów szyfrowania. Rozdział wieńczy opis uzyskanych wyników eksperymentalnych oraz porównanie pomiędzy wersjami bez kodów korekcyjnych oraz z kodami korekcyjnymi, otrzymując dane pozwalające sformułować podobne wnioski jak dla wersji o wysokiej wydajności.

W ostatnim rozdziale rozprawy doktorant podsumował wnioski z prac badawczych opisanych w drugiej części rozprawy oraz dokonał oceny proponowanych rozwiązań z perspektywy sprzętowej. Wyznaczono także potencjalne kierunki dla dalszych prac.

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 procesu standaryzacyjnego rozpoczętego przez amerykański Narodowy Instytut Standardów i Technologii (NIST) dotyczącego kryptografii postkwantowej.

Praca skupia się na dwóch aspektach kryptografii bazującej na kratach: efektywnym "łamaniu" krat (rozwiązywaniu problemów trudnych obliczeniowo) oraz efektywnym użyciu krat w kryptografii do zabezpieczania poufności informacji. Pierwszy aspekt pracy zrealizowany jest przez zaprezentowanie pierwszego według wiedzy autora, sprzętowego akceleratora przesiewania kraty - jednej z metod rozwiązywania znanego problemu trudnego obliczeniowo, zdefiniowanego na kratach.

Zaprezentowano nowatorską architekturę wraz z szczegółową analizą możliwości realizacji sprzętowej algorytmu przesiewania. Następnie przedstawiono zmodyfikowany równoległy algorytm GaussSieve, odpowiedni dla układów FPGA. Główny problem — komunikacja między układami CPU i FPGA — został rozwiązany za pomocą wspomnianego algorytmu, co pozwoliło osiągnąć niemal maksymalną możliwą akceleracje względem standardowych rozwiązań. Algorytm może być zaadoptowany do innych algorytmów przesiewania, które zwykle są pamięciowo-intensywne.

Na koniec części przedstawiono uzyskane rezultaty dla akceleratora i porównano je z wynikami osiąganymi przez implementację dedykowane na CPU. Co więcej, przedstawiono również porównanie kosztowe uruchomienia zaproponowanego rozwiązania w chmurze Amazon. Uzyskano znaczące przyspieszenie oraz oszczędności. Druga część pracy dotyczy jednego ze zgłoszeń na nowy postkwantowy algorytm szyfrowania oraz mechanizm enkapsulacji klucza, algorytm Round5. Algorytm został zaimplementowany dla układów programowalnych według dwóch założeń: maksymalnej przepustowości układu oraz niskiej zajętości (kosztem wydajności układu) rozwiązania. Obydwa rozwiązania różnią się

znacząco pod względem wydajności jak i zajętości układu. Osiągnięcie przedstawionych wyników było możliwe dzięki wykorzystaniu autorskiego projektu modułu mnożenia wielomianów obciętych.

Podsumowując tę część recenzji stwierdzam jednoznacznie, że moim zdaniem mgr inż. Michał Andrzejczak odpowiedział na postawione pytania i zrealizował 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. Autor rozprawy wybrał algorytm Gaussa przesiewania kraty jako przedmiot swoich badań. Jednakże jak sam autor opisuje w rozdziale trzecim, istnieją obecnie algorytmy przesiewania kraty cechujące się mniejszą złożonością obliczeniową, a więc też potencjalnie algorytmy szybsze i pozwalające odnaleźć rozwiązanie dla SVP w krótszym czasie. Jaka argumentacja stoi za tym wyborem? Czyż nie zasadniej byłoby przygotować algorytm o najmniejszej możliwej złożoności, by uzyskać narzędzie będące w stanie rozwiązać SVP w możliwie najkrótszym czasie? W jakim stopniu inne znane metody mogą wykorzystywać przedstawione w pracy mechanizmy?
2. Uzyskana przez autora akceleracja jest bardzo znacząca, jednakże w pracy nie przedstawiono żadnych rezultatów czasowych dotyczących rozwiązania SVP z wykorzystaniem opracowanego akceleratora. Co więcej, pomimo otrzymanych rezultatów autor nie znajduje się na liście najlepszych rezultatów w zakresie rozwiązywania SVP. Co miało wpływ na taki stan rzeczy?
3. W pracy porównywano wyniki dla dwóch platform sprzętowych: procesorów x64 oraz układów FPGA. Jednakże, dla pełnego obrazu stanu rzeczy brakuje odniesienia do kart graficznych. A zatem, jak w kwestii przesiewania sprawdzają się karty graficzne? Czy przedstawione metody mogą być również zaaplikowane do implementacji wykorzystujących GPU?
4. Algorytm Round5 nie został wybrany do dalszej rundy procesu standaryzacyjnego, jednak w pracy nie ma polemiki na temat powodów takiej decyzji.

Uwagi redakcyjne

Recenzowana praca doktorska napisana jest w języku angielskim. Język rozprawy jest co najmniej tak dobry jak mój i ewentualną ocenę mógłby zrobić być może *native speaker*. W części matematycznej nie znalazłem błędów. Niestety rzuca się w oczy wiele

niedociągnięć interpunkcyjnych, które oczywiście nie umniejszają wartości naukowej pracy, ale nieco rażą.

Wniosek końcowy

Przedstawione w recenzowanej rozprawie doktorskiej rozważania związane z konstruowaniem teoretycznych i praktycznych rozwiązań kryptografii postkwantowej opartych na kratach i problemach obliczeniowych z nimi związanych dotyczą ważnych i bieżących problemów kryptografii. Rozprawa doktorska mgra inż. Michała Andrzejczaka zawiera wiele oryginalnych oraz interesujących wyników. Moje uwagi polemiczne zawarte w recenzji nie zmniejszają mojej pozytywnej opinii o rozprawie jako całości.

Biorąc pod uwagę wyniki naukowe przedstawione w recenzowanej rozprawie doktorskiej mgra inż. Michała Andrzejczaka 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 mgra inż. Michała Andrzejczaka do dalszych etapów przewodu doktorskiego prowadzonego w dziedzinie nauk technicznych w dyscyplinie Informatyka przez Radę Dyscypliny Naukowej Informatyka Techniczna i Telekomunikacja Wojskowej Akademii Technicznej.