STRESZCZENIE ROZPRAWY DOKTORSKIEJ
„Acceleration of lattice based algorithms”

Michał Andrzejczak

Bieżący postęp w dziedzinie konstrukcji komputera kwantowego jest rosnącym zagrożeniem dla aktualnie stosowanej kryptografii klucza publicznego, podatnej na atak z wykorzystaniem algorytmu Shor'a. By zmniejszyć ryzyko ujawnienia poufnych informacji, zostały rozpoczęte prace badawcze nad bezpiecznymi konstrukcjami odpornymi na ataki z wykorzystaniem komputera kwantowego. Zwieńczeniem prac ma być ustanowienie nowych standardów jako efekt procesu standaryzacyjnego rozpoczętego przez amerykański Narodowy Instytut Standardów i Technologii (NIST).

Jedną z obiecujących dziedzin do realizacji nowych rodzajów szyfrów jest kryptografia bazująca na kratach. Niniejsza 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 akcelerację 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. Dla obydwu wersji porównano wpływ wykorzystania kodów korekcyjnych na wyniki implementacji sprzętowej.

ABSTRACT OF PHD THESIS
„Acceleration of lattice based algorithms”

Michał Andrzejczak

The ongoing development of quantum computers is a rising threat for currently used public key cryptography, vulnerable to Shor's algorithm. To mitigate the risk of secret data being revealed, research works on ciphers, secure against quantum computers, have been performed, which lead to a new standardization process announced by the U. S. NIST. One of the promising fields for modern secure ciphers is lattice based cryptology. This work focuses on two aspects of lattices: how to efficiently 'break' them and how to efficiently use them.

The first aspect is done by developing the first reported so far in the literature, an FPGA accelerator for lattice sieving algorithms - a method for solving one of the major hard computational problems defined over lattices, the SVP. A novel architecture for lattice sieving and detailed analysis of hardware capabilities for sieving is presented. Then, a new modified parallel approach for *GaussSieve*, suitable for FPGAs, is presented. The main issue - communication between CPU and FPGA - is resolved with a new algorithm that allows it to reach almost maximal possible acceleration. The algorithm can be adopted to other sieving-like algorithms, which usually are memory intensive. At the end, the performance results are presented and compared to a standard CPU. Moreover, the proposed solution is also cost-compared using AWS. Significant speed-up and savings are achieved.

In the second part of this thesis, one of the proposals for a new standard for public key encryption and key encapsulation mechanism, *Round5* is implemented in hardware. Two approaches for digital design are presented. The first one is aimed at achieving the best performance possible, while the second one is targeted to be a low resource utilizing module, able to be deployed on the smallest devices. Both designs vary in terms of performance and resource utilization. The results were obtained with a novel truncated polynomial multiplier. For both designs the influence of error correcting codes for hardware performance was measured and compared.