Катедри за рачунарство и информатику
Предмет: Сагласност за одбрану мастер рада.-

Одлуком Катедре и ННВ од 30.6.2017. именовани смо у комисију за одбрану мастер рада под насловом "Имплементација неких алгоритама на квантним рачунарима" кандидата **Николе Спасојевића,** студијски програм Информатика.

Никола Спасојевић је 20.9.2019. доставио текст свог рада, чија тема су квантни рачунари и алгоритми за ове рачунаре, између осталог и алгоритми који угрожавају сигурност неких криптографских алгоритама који се данас широко примењују. Пост-квантна криптографија је данас посебна област криптографије, настала као одговор на појаву квантних рачунара. У раду је изложен увод у квантну механику и неопходни елементи за разумевање квантних рачунара. Детаљније је описано неколико алгоритама за квантне рачунаре заснованих на квантној Фуријеовој трансформацији.
Рад је подељен у седам поглавља. У уводу се излаже мотивација за избор ове теме и захтеви о којима се водило рачуна приликом писања текста - да рад буде концизан и разумљив информатичарима, тако да за размевање рада није неопходно дубље знање математике, као ни било какво знање из квантне механике. У другом поглављу се излажу неопходни појмови из квантне механике, суперпозиција и уплетеност. У трећем поглављу се најпре излажу неопходна знања из линеарне алгебре и квантне механике, а затим неопходни основни појмови о постулатима квантне механике, мешаним стањима, квантној телепортацији, супергустом кодирању и физичкој реализацији квантних рачунара. У четвртом поглављу предност квантних над обичним рачунарима приказана је на примеру Дојч-Јоза алгоритма за проверу да ли је задата Булова функција од *n* променљивих константна или балансирана. У петом поглављу описују се квантни алгоритми засновани на Фуријеовој трансформацији - Шурови алгоритми за факторизацију и решавање проблема дискретног логаритма. Разматрају се последице постојања ова два алгоритма, с обзиром да се већина модерних криптографских алгоритама са јавним кључем заснива на тежини решавања једног од ова два проблема. После шестог поглавља у коме се описује утицај квантних рачунара сада и у будућности, следи закључак рада.

Мишљење.

Увидом у текст **Николе Спасојевића** "Програмска Имплементација неких алгоритама на квантним рачунарима" дошли смо до закључка да приложени рад задовољава у потпуности захтеве који се постављају при изради мастер рада и предлажемо Катедри да одобри јавну одбрану рада.

У Београду, 4.10.2019.

Др Миодраг Живковић, ред. проф., ментор

Др Саша Малков, ванр. проф.

Др Анђелка Ковачевић, ванр. проф.

Др Александар Картељ, доцент