Универзитет у Београду – Математички факултет
Наставно-научном већу

ИЗВЕШТАЈ

Одлуком Наставно-научног већа Математичког факултета одређени смо у комисију за преглед и оцену докторске дисертације Хане Алмонер Лоуке (Hana Almoner Louka) под насловом «Квантна теорија информација и асимптотика квантног потписивања уговора». После прегледа рукописа, подносимо овај извештај.

Рукопис је сложен на рачунару, има 64 странице и следећа поглавља: 1. Увод у квантну механику, 2. Квантна теорија информација, 3. Криптографија и потписивање уговора, 4. Асимптотика квантног потписивања уговора, 5. Референце. Литература на крају рада садржи 52 библиографске јединице.

Садржај дисертације

Предмет изучавања у овој дисертацији је квантна теорија информација, и специјално протоколи квантног потписивања уговора.

У тези је најпре дат приказ основа квантне механике са релевантим математичким апаратом. Потом је дат осврт на квантне алгоритме, и детаљно су објашњени Шоров и Гроверов алгоритам. Затим је дат осврт на класичну криптографију, и нека квантне криптографске протоколе, попут ББ84 квантне расподеле кључева. Потом је приказан протокол квантог потписивања уговора базиран на раду N. Paunković, J. Bouda, and P. Mateus, "Fair and optimistic quantum contract signing", Physical Review A (2011).

Циљ истраживачког дела дисертације био је да се испита протокол квантног потписивања уговора, дат у раду Paunković-Bouda-Mateus. Суштински услов асимптотске скоро сигурне коректности у том раду је испитан нумерички, али није доказан аналитичким путем.

У дисертацији је доказана хипотеза из поменутог рада о асимптотском понашању вероватноће варања (Теореме 7,8 и 9 из тезе). Такође, показано је да је рандомизација по параметру α у протоколу неопходна, да би вероватноћа варања тежила нули (Теорема 6).

Дисертација, писана на енглеском језику, садржи следећа поглавља и подпоглавља:

Глава 1, која је уводног карактера, садржи дефиниције и особине основних појмова из квантне механике, који се користе у тези, као и релевантни математички апарат. Дати су постулати квантне механике, описани су корелисани и некорелисани вектори, ЕПР парови, важни у квантој теорији информација, као и уведена нотација која се користи у овој области. Дата је и једноставна илустрација Белових неједнакости на примеру ЕПР пара.

Глава 2 садржи преглед квантне теорије информација. Објашњени су квантни алгоритми, Шоров алгоритам растављања бројева на чиниоце као и Гроверов алгоритам квантног претраживања, и дати примери. Такође је објашњен сам појам квантих кола, уз преглед елементарних операција на једном, два и три кубита. Код Шоровог алгоритма, објашњен је и алгоритам за налажење периода, заснован на дискретној Фуријеовој трансформацији која се код квантних рачунара може добити у времену полиномијалном у односу на логаритам дужине низа.

У глави 3 изложене су основе криптографије, класични РСА алгоритам као и класична теорија потписивања уговора. Описан је и квантни алгоритам ББ84 за дистрибуцију кључева, који се заснива на корелисаним ЕПР паровима кубита (Белова стања).

Глава 4 садржи резултате везане за асимптотику квантног потписивања уговора. Описан је протокол Паунковић, Бауда и Матеуса, заснован на корелисаним ЕПР паровима кубита, који не зависи од дигиталних потписа. Доказано је неколико оригиналних резултата везаних за асимптотику вероватноће варања и неопходност рандомизације параметара у протоколу.

Најзад, на крају рада дат је преглед литературе, који садржи 52 библиографске јединице.

У дисертацији се користе методе математичке анализе, али и методе кванте теорије информација. Добијени резултати су основа неколико научних радова кандидата.

1. Hana Almoner Louka, "Polynomial equations – from ancient to modern times – a review", Zilten (University Bulletin), Issue 16, Vol 2, Libija, 2014.
2. Vladimir Božin, Hana Louka, Asymptotics of quantum contract signing, Publications de l'Institut Mathématique
3. Hana Louka, Necessity of Parameter Randomization in Quantum Contract Signing, Matematički vesnik
4. Vladimir Božin, Hana Louka, On quantum contract signing protocol, (Filomat)

Закључак

Предложена теза је занимљива и актуелна и представља даљу разраду и разјашњење протокола из рада Paunković-Bouda-Mateus. Резултати ове дисертације разјаснили су асимптотику за случај великог броја кубита, и показали хипотезу о вероватноћи варања. Показана је и неопходност рандомизације параметара, уз експлицитну стратегију за варање у случају када рандомизације нема. Такође, дат је преглед квантне теорије информација, која представља активну истраживачку област.

С обзиром на изложено у овом Извештају, Комисија предлаже Наставно-научном већу да прихвати овај извештај, одобри одбрану докторске дисертације и одреди комисију за одбрану кандидата Хане Алмонер Лоуке.

У Београду, августа 2016.

_____

др Владимир Божин, доцент, ментор

_____

др Милош Арсеновић, редовни. проф.

_____

др Александар Липковски, редовни проф.

_____

др Никола Паунковић, математички департман, Универзитет у Лисабону