Становище

по процедура за публична защита на дисертационен труд на тема:
"Конструиране на булеви функции и цифрови последователности за криптологията и комуникациите"
за придобиване на образователна и научна степен "Доктор"
от Мирослав Маринов Димитров

Област на висше образование: 4. Природни науки, математика и информатика,
Професионално направление: 4.6. Информатика и компютърни науки,
Докторска програма: "Информатика",
секция: "Математически основи на информатиката" (МОИ),
Институт по математика и информатика (ИМИ),
Българска Академия на науките (БАН)

Становището е изготвено от проф. д-р Мая Митева Стоянова, заместник-декан на Факултета по математика и информатика, СУ "Св. Климент Охридски", катедра "Алгебра", 4.5. Математика (РАС), в качеството ми на външен член на научното жури, съгласно Заповед 521/02.12.2022 г. на Директора на ИМИ, БАН и решение на Научното жури (Протокол 1/06.12.2022 г.).

1 Обща характеристика на дисертационния труд и представените материали

Представеният дисертационен труд е на английски език и е в обем от 212 страници. Състои се от увод, четири глави, 2 части - приложения и библиография от 152 заглавия. В приложения (разширен) автореферат на български език, в рамките на 59 стр., е представено в резюме съдържанието на дисертацията, като ясно и точно са отразени както основните приноси на докторанта, така и къде са апробирани резултатите. Дисертационният труд се базира на резултати, публикувани в седем публикации и на две подадени за публикуване и налични в arXiv препринта. Представените материали и документи от докторант Мирослав Димитров удостоверяват, че са спазени всички изисквания на Закона за развитие на академичния състав в Република България (ЗРАС в Република България) и правилниците към него. От публикациите на Мирослав Маринов Димитров е видно, че отговаря и

многократно надхвърля минималните национални изисквания на чл. 2б. ал. 2 и ал. 3 от ЗРАС в Република България за придобиване на образователна и научна степен "доктор".

2 Данни и лични впечатления за кандидата

Познавам Мирослав Димитров и научната му работа от Националния семинар по Теория на кодирането "Проф. Стефан Додунеков". От лични разговори с научния му ръководител проф. дн Цонка Байчева знам, че имат отлични професионални работни взаимоотношения като научен ръководител и докторант, което е видно и от представените от тях (в дисертационния труд на докторант М. Димитров) съвместни научни резултати.

Мирослав Маринов Димитров придобива ОКС "Бакалавър" във Факултета по математика и информатика на Софийски университет "Св. Климент Охридски", специалност "Математика" през 2009 г. През 2016 г. придобива ОКС "Магистър" във Факултет по математика и информатика на Софийски университет "Св. Климент Охридски", магистърска програма "Защита на информацията в компютърните системи и мрежи". От 05.07.2017 г. е зачислен като задочен докторант към докторска програма "Информатика" в секция МОИ, ИМИ, БАН. Със Заповед 619/30.06.2021 г. е отчислен с право на защита. От 2017 г. до момента Мирослав Димитров е експерт към ДАНС в Република България.

3 Съдържателен анализ на научните и научно-приложните постижения на кандидата, съдържащи се в представения дисертационен труд и публикациите към него, включени по процедурата

В дисертацията се разглеждат различни стратегии за конструиране и анализ на булеви функции, C-кутии и цифрови редици.

Във втора глава са включени необходимите дефиниции и означения, както и подробно са анализирани някои популярни C-кутии. В Глава 3 се разглежда стратегия за намиране на аномалии в структурите на C-кутиите чрез използването

на спектрален анализ. Глава 4 е изцяло ориентирана към PSL проблема. В Глава 5 се разглежда MF проблема.

Основните научни приноси на докторант Мирослав Димитров в представената дисертация са:

1. Подробно е анализирана богата колекция от популярни векторни булеви функции като е демонстрирано, че една голяма част от векторните булеви функции построени посредством функции от теория на хаоса са уязвими на линеен криптоанализ. Предложен е ефикасен алгоритъм, който достига до значително по-добри характеристики от тези, които авторите на гореспоменатите векторни булеви функции използват за сравнение.

2. Въведени са нови помощни структури и дефиниции, като куплунги, декомпозиция по координати и CELAT таблица, които позволяват формулирането на проблема по нелинейната оптимизация на булеви функции като фамилия от SAT проблеми. Открити са 8×8 биективни векторни булеви функции, съставени от координати с нелинейност 116.

3. Предложена е стратегия за спектрален анализ на векторни булеви функции за откриване на аномалии, както и ефикасен евристичен алгоритъм за конструиране на двоични редици с малки пикове на страничните апериодични автокорелационни листове (PSL). Намерени са рекордни PSL стойности за дължини на редици между 106 и 300. Предложено е подобрение на гореспоменатия алгоритъм за свеждане на времевата сложност и изискуемата памет до линейни стойности. Направените модификации позволяват достигането на рекордни PSL стойности за по-малко от секунда, дори и при редици с по-големи дължини.

4. Направен е подробен анализ и сравнение на ефикасността на алгоритмите при различни входни параметри, което довежда до създаването на нов алгоритъм за достигнане до оптималните PSL стойности за известните от литературата дължини, които са открити след пълно обхождане.

5. Предложен е алгоритъм за видео ускорители, който е насочен към намиране на оптимални PSL стойности измежду дадена двоична редица B и всички нейни възможни ротации. Намерени са всички PSL оптимални m-редици, с или без ротации, за дължини $2^n - 1$, за $n = 18, 19, 20$. Намерени са и всички PSL оптимални редици на Legendre, с или без ротации, до дължини 432100. Резултатите водят до предположението, че всички PSL оптимални редици на Legender, с или без ротации, и за дължини N по-големи от 235723, притежават PSL стойност строго по-голяма от $\sqrt{N}$.

6. Предложени са няколко подобрения на водещите алгоритми за конструиране на изкривено-симетрични (skew-symmetric) двоични редици с ниски качествени

стойности (MF), които редуцират сложността по памет от n^2 до n, без това да повлиява на времевата им сложност. Предложен е и алгоритъм, който оптимизира случайно генерирани изкривено-симетрични двоични редици с дължини до 10^5+1 и MF стойности строго по-големи от 5. Това противоречи на предположението на Bernasconi, че няма да бъде създадена стохастична процедура, която да намира двоични редици с дължини над 200 и MF стойности над 5.

7. Предложени са нови класове двоични редици с четни дължини и алтернират автокорелационни странични листи равни на 1 по абсолютна стойност. MF стойностите на предложения клас редици са близки до MF стойностите на изкривено-симетричните редици открити от Golay. Предложени са подкласове от редици, базирани на проблема с разбиването на числа. Открити са двоични редици с рекордни MF стойности за много от дължините до 225 и за всички дължини над 225. Като допълнителна демонстрация за ефикасността на предложения алгоритъм, е направен сравнителен анализ между водещите алгоритми и представения в дисертацията алгоритъм върху двоични редици с дължини 573 и 1009. Предложена е нова стратегия за спектрален анализ на векторни булеви функции посредством апериодични автокорелационни функции.

Преставените по-горе резултати ми дават основание да твърдя, че кандидатът Мирослав Маринов Димитров има задълбочени познания в тематиката на дисертационния труд, както и че оригиналните му приноси са повече от достатъчни за придобиване на ОНС "Доктор".

4 Апробация на резултатите

От представените документи е видно, че докторант Мирослав Димитров е оформил своя дисертационен труд въз основа на резултати, публикувани в седем публикации и две подадени за публикуване и налични в arXiv препринта. Три от публикациите са самостоятелни, както и двата препринта. От останалите четири публикации, три са в съавторство с научния му ръководител проф. дн Цонка Байчева и д-р Николай Николов, а последната публикация е в съавторство с М. Илиев, Н. Николов и Б. Беджев. Две от публикациите, публикувани през 2020 г., са в IEEE Signal Processing Letters, IF : 3.109 (2020) и втори квартил Q_2 (2020) в Web of Science, които (съгласно Правилника за прилагане на ЗРАС в Република България за ПН 4.6. Информатика и компютърни науки) носят на кандидата по 60 точки всяка; три от статиите, публикувани както следва: една през 2020 г. и две през 2021 г., са в IEEE Access, IF : 3.367 (2020) и втори квартил Q_2 (2020) в Web of Science и IF : 3.476 (2021) и втори квартил Q_2 (2021) в Web of Science,

съответно като носят на кандидата по 60 точки всяка; шестата публикация от 2020 г. е в IEEE Communications Letters, IF : 3.436 (2020) и втори квартил Q_2 (2020) в Web of Science и носи на кандидата 60 точки; седмата публикация е в тома на 2020 International Conference on Information Technologies (InfoTech), който е реферирaн в Scopus и IEEE Xplore и носи 18 точки. В резултат с общо 378 точки (при необходими 30 т.) кандидатът Мирослав Димитров покрива и многократно надвишава минималните национални изисквания по чл. 2б, ал. 2 и 3 на ЗРАС в Република България, изискуеми за придобиване на ОНС "Доктор" в ПН 4.6. Информатика и компютърни науки. Нямам информация и каквито и да било съмнения за плагиатство в представения дисертационен труд и научни трудове по тази процедура. До момента има 45 цитирания на публикациите.

5 Качества на автореферата

Представените автореферати, съответно на български и на английски език, са в обем от 59 страници, като и двата са изготвени съгласно всички изисквания и отразяват коректно съдържанието на дисертационния труд и научните приноси на докторанта.

6 Критични бележки и препоръки

Нямам критични бележки.

7 Заключение

След като се запознах с представените в процедурата дисертационен труд и придружаващите го научни трудове и въз основа на направения анализ на тяхната значимост и съдържащи се в тях научни и научно-приложни приноси, **давам своята положителна оценка и потвърждавам**, че представеният дисертационен труд и научните публикации към него, както и качеството и оригиналността на представените в тях резултати и постижения, отговарят на изискванията на ЗРАС в Република България, Правилника за приложението му и съответните правилници на ИМИ и на БАН за придобиване от кандидата на образователната и научна степен "Доктор" в област на висше образование 4. Природни науки, математика и информатика, професионално направление 4.6. Информатика и компютърни науки. В частност кандидатът удовлетворява минималните национални изисквания

в професионалното направление и не е установено плагиатство в представените по процедурата научни трудове.

Въз основа на гореизложеното, **убедено препоръчвам** на научното жури да присъди на Мирослав Маринов Димитров образователна и научна степен "Доктор" в област на висше образование 4. Природни науки, математика и информатика, професионално направление 4.6. Информатика и компютърни науки, докторска програма "Информатика", секция МОИ, ИМИ, БАН.

10.01.2023 г.
гр. София

Подпис:
проф. д-р Мая Стоянова