СТАНОВИЩЕ

по процедура за придобиване на научна степен "доктор" в

област на висше образование: 4. **„**Природни науки, математика и нформатика”,
професионално направление: 4.6 „Информатика и компютърни науки“.

Автор: **Мирослав Маринов Димитров**, задочен докторант в секция „Математически основи на информатиката“, ИМИ – БАН.

Тема: ”Конструиране на булеви функции и цифрови последователности за криптологията и камуникациите”.

Становището е изготвено от **проф. дн Цонка Стефанова Байчева**, Институт по математика и информатика, БАН, област на висше образование 4. Природни науки, математика и информатика, в качеството ми на член на Научното жури съгласно Заповед № 521/2.12.2022 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

В дисертацията са разработени методи за конструиране на векторни булеви функции и цифрови последователности с най-добри до момента по отношение на някои техни основни параметри стойности. Компютърните имплементации на разработените методи имат много добри характеристики по отношение на използвана памет и времева сложност, като някои от тях използват ефективно възможностите на паралелното изпълнение или съвременните видео ускорители. С разработения софтуер е направен анализ на богата колекция от използвани в различни приложения векторни булеви функции, построени са 8x8 векторни булеви функции съставени само от координати с нелинейност 116, конструирани са двоични редици с малки пикове на страничните апериодични автокорелационни листове (PSL) и с големи качествени стойности (MF). Предложени са различни стратегии за спектрален анализ на векторни булеви функции за откриване на аномалии.

Дисертационният труд е написан на английски език, съдържа 212 страници като 56 от тях са приложение с таблици с получени резултати. Цитираната библиография включва 152 заглавия.

Мирослав Маринов Димитров е представил всички изискуеми документи, съгласно ЗРАС в Република България, Правилника за прилагането му и съответния Правилник за придобиване на научни степени и заемане на академични длъжности на ИМИ, БАН. Представените документи показват, че кандидатът отговаря на минимални национални изисквания на ЗРАС в Република България.

2. Данни и лични впечатления от кандидата

Мирослав Маринов Димитров е завършил магистърска степен във ФМИ на СУ „Св. Климент Охридски“ през 2016 година. От 2017 година работи като експерт в ДАНС и е задочен докторант в ИМИ-БАН. Отчислен е с право на защита със заповед № 619/30.06.2021 година.

Мирослав Димитров имаше много сериозна предварителна подготовка по тематиката на докторантурата, която значително обогати и развви по време на докторантското си обучение. Той е много мотивиран, отговорен, а заради добрата си фундаментална подготовка по математиката и информатиката навлиза бързо в нови изследователски задачи. По време на докторантурата си, участва в 4 престижни международни състезания по киберсигурност и се класира на челни места, както и стана съавтор на две глави от електронен учебник CryptoTool Book. Показа и умения за самостоятелна работа.

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

Дисертационният труд се състои от увод представящ научните приноси на докторанта, публикациите по дисертацията и техните цитирания, пет глави, литература и приложение.

Глава първа е въведение, в което са описани различните приложения на изследваните в дисертацията комбинаторни обекти и техните основни характеристики, които са от значение за използването им в криптологията и комуникациите. Обобщени са известните до момента резултати за тези характеристики и са коментирани използваните за получаването им методи. Направен е кратък преглед на съдържанието на следващите четири глави от дисертацията.

Във втора глава са разгледани векторните булеви функции от гледна точка на тяхното приложение в криптографията. Дадени са дефинициите и означенията, които се използват в следващите секции и глави. Подробно са анализирани криптографските свойства на богат набор от популярни С-кутии. Обобщени са известните стратегии за конструиране на С-кутии с добри криптографски свойства и са класифицирани в четири категории. Специално място е отделено на векторни булеви функции, конструирани чрез използване на теория на хаоса и е предложен ефективен алгоритъм, който подобрява всички получени до момента резултати. Направено е много важното уточнение, че другите автори, предлагащи подобни конструкции, оптимизират само нелинейността на координатите на С-кутията, като игнорират техните линейни комбинации. По този начин, общата нелинейност на тези кутии е значително по-ниска и те са силно уязвими към линеен криптоанализ. Въведени са нови понятия и характеристики на С-кутиите, които позволяват формулирането на задачата за оптимизация на тяхната нелинейност като задача за удовлетворимост, която може да се

реши чрез използването на SAT solvers. Предложеният алгоритъм постига увеличаване на нелинейността на С-кутията чрез минимални промени в нейната структура, като така оптимизацията се фокусира върху нейните слаби елементи без да се намаляват добрите характеристики на останалите елементи. Така е построена балансирана С-кутия с размери 8x8 с нелинейност на координатите 116 и обща нелинейност 92.

В трета глава се разглежда стратегия за намиране на аномалии в структурите на С-кутиите чрез използването на спектрален анализ. Наличието на аномалии може да позволи на създателите на кутията да прилагат известни само на тях атаки, да ги използват за ефективната им хардуерна имплементация или дори да внедряват в тях зловредни структури. Направен е спектрален анализ на голяма колекция от популярни С-кутии като резултатите са графично илюстрирани. Показано е, че процесът на спектрален анализ може да се автоматизира и да се приложи не само за линейната апроксимираща (LAT) таблица, но и за други таблици като DDT, ACT, XOR.

В четвърта глава е разгледана задачата за определяне на максималната стойност на страничен лист (PSL) на двоична редица с ниска автокорелация. Заради разнообразните им практически приложения тези редици са широко изследвани и са разработени различни методи за тяхното генериране. Определени са оптималните стойности на PSL за двоични редици с дължини до 84. В дисертацията е предложен бърз и лесен за имплементиране евристичен алгоритъм за конструиране на двоични редици с ниски PSL стойности, с който са изследвани двоичните редици с дължини между 106 и 300. За 95 от тях са намерени такива с по-добри стойности от известните до момента. Алгоритъмът може да се използва и за конструиране на редици с дължини по-големи от 300. Разработен е метод за конструиране на редици с големи дължини и малки PSL стойности, който има линейни сложности по време и по памет. Имплементацията на метода е сравнена с колекция от известни в литературата алгоритми като за всички тествани дължини се получават редици с по-добри PSL стойности, като в някои случаите това се постига за по-малко от секунда. Направени са сравнения и за дължини над 2^{12} като са използвани m-редици, които съществуват само за дължини 2^n-1 и, за които има известни резултати. За всички тествани дължини за n между 13 и 17 са получени по-добри стойности на PSL. Разгледана е и задачата за намиране на най-ниската PSL стойност измежду дадена редица B и всички възможни нейни ротации. Показано е, че ако се използват някои математически свойства на тези редици, задачата може да се реши от перфектно балансиран паралелен алгоритъм. Чрез пълно обхождане са пресметнати оптималните PSL стойности на m-редиците с дължини 2^n-1 за n=18,19 и 20, както и на всички редици на Legendre, с и без ротация, с дължини до 432100.

В пета глава се разглежда задачата за конструиране на цифрови редици, чиято апериодична автокорелация е колективно малка по отношение на някаква подходяща мярка. Една такава мярка е merit factor (MF) и определянето на най-голямата стойност на MF за дълги двоични редици е задача, разглеждана от десетилетия в комплексния

анализ и комбинаторната оптимизация. В тази глава са изведени някои свойства на изкривено-симетричните двоични редици и са използвани за намаляване от квадратична до линейна на сложността по памет на известните алгоритми за конструиране на такива редици без да се променя времевата им сложност. Предложен е алгоритъм, който оптимизира случайно генерирани изкривено-симетрични двоични редици с дължини до 10^5+1, до такива с MF > 5. Така е опровергано предположението на Bernasconi, че няма да бъде създадена стохастична процедура, която да намира двоични редици с дължина над 200 и MF > 5. За четни дължини, където не може да има изкривено-симетрични двоични редици, са въведени псевдо изкривено-симетрични двоични редици със стойности на MF близки до тези на изкривено-симетричните редици, открити от Golay. Предложени са и редици породени от задачата за разбиване на числа, които подобряват известните стойности на MF за много от редиците с дължини до 255 и за всички с дължини над 255. Алгоритъмът за конструиране на такива редици е изключително ефективен и за няколко часа води до конструирането на редици, за които с други от известните алгоритми биха били необходими от десетки до милиарди години. В последния раздел на главата е предложена стратегия за откриване на скрити вътрешни връзки между координатите на C-кутия като се визуализират страничните листи на всевъзможните линейни комбинации от двойките координати съставящи C-кутията.

4. Апробация на резултатите

Дисертацията е написана въз основа на 9 труда. Те са публикувани или поставени в arXiv както следва:

- 6 в международни списания с импакт фактор,
- 1 в сборник на международни конференция реферирaн в Scopus и IEEE Xplore,
- 2 в arXiv.

Три от публикациите по дисертацията са написани в съавторство с научния ръководител на докторанта, а една от тях е с други трима съавтори. Останалите пет публикации са самостоятелни като три са публикувани в издания с импакт фактор, а две в arXiv. В качеството ми на научен ръководител на докторанта, определям приноса му в съвместните публикации като равностоен на този на неговите съавтори. Броят и качеството на трудовете, върху които е написана дисертацията, са в съответствие с минималните национални изисквания за придобиване на образователната и научна степен "доктор".

До 20.11.2022 година са забелязани 45 цитирания на публикациите, върху които е написана дисертацията, като 35 от цитиранията са в издания с импакт фактор, 5 са на международни конференции, 4 в дисертации в чужбина и 1 в препринт.

5. Качества на автореферата

Авторефератът на български език е в обем от 58 страници и дава ясна и адекватна представа за съдържанието и основните резултати на дисертацията. Авторефератът на английски език в обем от 59 страници и представя точно резултатите от дисертационния труд и неговото съдържание.

6. Заключение

След като се запознах с представените по 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, 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 ЗРАСРБ, Правилника за приложението му и съответния Правилник на ИМИ-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 дисертация и научни трудове.

Въз основа на гореизложеното, **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.

10.01.2023 г. Подпис:

/проф. дн Ц. Байчева /