**РЕЦЕНЗИЯ**

по дисертационен труд за присъждане
на образователна и научна степен „доктор“

**Тема**: „Конструиране на булеви функции и цифрови последователности за криптологията и комуникациите“

**Автор**: Мирослав Маринов Димитров,
Секция „Математически основи на информатиката“ (МОИ), Институт по Математика и информатика, Българска академия на науките

**Научен ръководител:** проф. д.м.н Цонка Стефанова Байчева

**Научна област:** 4. Природни науки, математика и информатика

**Професионално направление:** 4.6. Информатика и компютърни науки

**Изготвил становището**: проф. дмн Николай Иванов Янков – ШУ „Епископ К. Преславски”

Със заповед № 521/02.12.2022 г. на Директора на Института по математика и информатика (ИМИ) при БАН съм назначен за член на Научното жури по процедурата и на първото заседание на това жури съм избран за изготвянето на настоящата рецензия. Предоставени са ми всички материали в съответствие с изискванията на нормативните документи, които са редовни и съответстват на ЗРАСРБ. Нямам информация за нарушения по процедурата, не ми е известно в дисертацията да има плагиатство.

1. **Данни за дисертанта**

Дисертантът Мирослав Димитров има диплома от 2009 г. ОКС „бакалавър“ в СУ „Св. Климент Охридски“ в направление информатика. През 2016 г. получава магистърска степен от същия университет в образователната програма „Защита на информацията в компютърните системи и мрежи“. В приложената към документацията оскъдна автобиография, за съжаление, няма данни за участието му в научни проекти. В списъка с участия в научни форуми са вписани два доклада: на OCRT'17 в София и CRYPTACUS в Португалия през 2018.

2. **Данни за докторантурата**

Докторантът е зачислен в задочна форма на обучение от 05.07.2017 г. с период на обучение 4 г. и отчислен с право на защита с решение на НС на ИМИ (Протокол № 619/30.06.2022 г.). Предварителното обсъждане на дисертацията, на което присъствах, се състоя на 11.11.2022 г. на разширено заседание на секция МОИ в рамките на националния семинар по кодиране „Проф. С. Додунеков“. Със заповед

на директора на ИМИ е определено научно жури и датата на защитата. Считам, че процедурата е редовна и няма нарушения.

### 3. Данни за дисертацията и автореферата

Представения за рецензия дисертационен труд е написан изцяло на английски език и се състои от: увод (6 стр.), основен текст (116 стр.) от 5 глави, разделени на секции. В дисертацията е включен списък с приносите, литература от 152 заглавия, както и списъци с диаграмите, таблиците и алгоритмите. Трудът отговаря на изискванията на Закона за развитие на академичния състав в РБ (ЗРАСБ) и правилника за приложение на ЗРАСРБ (ППЗРАСРБ), както и на Правилника за условията и реда за придобиване на научни степени и за заемане на академични длъжности в БАН (ПБАН). Авторефератът в обем от 59 стр. отразява адекватно основните идеи и съществените крайни резултати, които са описани в дисертационния труд.

Макар че по ЗРАСРБ не се изискват цитирания, считам за показателен факта, че към дисертацията са приложени 45 забелязани цитирания, от които повече от половината: 25 са от последната година. Това разкрива големия потенциал на представената дисертация, както е и отлично признание от международната общност на значителните научни приноси на труда.

### 4. Общо описание на дисертацията

В глава 2 на дисертацията са разгледани възможните стратегии за конструиране на C-кутии: $T_1$ – псевдослучайна генерация; $T_2$ – алгебрични конструкции или друг детерминистичен подход; $T_3$ – евристични методи за търсене на решение, оптимизиращо псевдослучайна кутия; $T_4$ – подход на хибридно търсене. Намерен е нов алгоритъм основан на стохастичен hill climbing метод, при който е предложено условието за спиране да е достигането на $\frac{n(n-1)}{4}$ цикъла.

С помощта на този алгоритъм е постигната максималната известна към момента стойност на средна координатна нелинейност (ACNV) от 114,5. Така се доказва, че структурата (в случая използвайки евристични методи с начало псевдослучайни C-кутии) дава по-добри резултати, отколкото когато се използват хаотични функции. Това не е изненада за повечето изследователи, които в практиката се сблъскват с това, че случайните и/или хаотични структури рядко са оптимални. В §2.5. е показано, че задачата за намирането оптимални откъм характеристиката нелинейност C-кутии може да бъде сведена до стандартна задача за бинарно оптимизиране, която е добре изучена и имплементирана в повечето CAS приложения. Това свеждане се осъществява чрез промяна на стойностите на два бита от C-кутията. Въведени са нови понятия: сдвояване, опорно множество за

сдвояване, координатна декомпозиция и други, с чиято помощ е доказана връзката с решима задача от двоичното целочислено линейно програмиране (BILP), при която не се търси оптималното решение – бит, а само едно от възможните решения. Като приложение са анализирани две стандартни С-кутии – Skipjack (САЩ) $S_k$ и Кузнечик $K_k$ (стандартизиран симетричен криптографски алгоритъм за РФ) и използвайки новополучения алгоритъм нелинейността и на двете е подобрена от 100 на 102. За $S_k$ промяната се състои в 4 бита, а за $K_k$ в 12 (от 2048). Стартирайки оптимизационния процес от С-кутията с размери 8x8, която има най-голямата досега известна средна координатна нелинейност (ACNV) 114,5 се достига до кутия, която има ACNV стойност 116 и обща нелинейност от 92.

Трета глава на дисертацията е относително по-приложна. В нея е извършено надграждане на работите на Aleksei Udovenko и Leo Perrin (включително и докторската му дисертация от 2017 г.) за използването на спектрален анализ на С-кутии с помощта на линейно приближение, разпределение на разликата и автокорелационни таблици. С помощта на предложената визуализация (оцветяване в червено само на тези елементи, отговарящи на избраното ограничение) могат да се забележат симетрии и аномалии, които евентуално биха улеснили или спомогнали евентуалното разбиване на С-кутията. Подбирайки подходящи спектри са показани необясними структури в голяма част от известните С-кутии. Предложен е начин за автоматизиране на процеса за намиране на аномалии, включително и използвайки и други характеристики на С-кутиите като: таблица за разпределение на разликата (DDT), таблица на автокорелациите (ACT) и XOR таблица (XORT).

В глава 4 е посветена на двоичните последователности. Предложен е нов shotgun hill climbing алгоритъм за намиране на оптимални откъм нивото на максималния страничен лист (PSL) последователности. Този алгоритъм намаля сложността откъм време за изпълнение и памет до нива $O(n)$. С негова помощ са генерирани по-дълги двоични $m$-последователности, които имат рекордни PSL стойности. Показано е и приложение на алгоритъма към завъртени Лежандрови последователности. Поради намаляването на нужната памет за работата на алгоритъма за намаляване на PSL, предвид и това че той е паралеризируем е извършена негова имплементация за CUDA архитектура, при това се изследват едновременно всички ротации на последователността. Показано е значително увеличение на скоростта и намаление на нужната памет, в сравнение със стандартни алгоритми като например този в NymPi. Всички $m$-последователности с дължина $2^n - 1, n \in \{18, 19, 20\}$ са успешно обходени. В резултата на тези подобрения, значително е улеснена и задачата за намирането на всички оптимални Лежандрови

последователности до дадена дължина. В дисертацията тази задача е решена за дължини ≤ 432100.

Последната глава 5 на дисертационния труд е посветена на считаната за една от най-трудните оптимизационни задачи – намирането на начин да се увеличи качествения фактор (MF) на двоичните последователности за дадена дължина. Чрез използването на flip операция е подобрен алгоритъма за оптимизиране на MF на последователности: При дадена косо-симетрична последователност $L$ с нечетна дължина, при промяна на елементите в позиции $q$ и $n-q-1$ за дадено $q$ се получава нова последователност $L^q$, която запазва свойството косо-симетричност. Получени са 6 свойства на $L^q$ (Теорема 5.1.1), които позволяват да се получи разбиване на множеството от събираеми и да се опрости формулата. Новата версия на алгоритъма реализира намаляване на паметта от $O(n^2)$ на $O(n)$, при това без да се намаля бързодействието му. Намерени са множество косо-симетрични двоични последователности с $MF > 5$. Показан е нов клас от двоични псевдо-косо-симетрични последователности с големи дължини (до $10^5+1$).

## 5. Научни и научно-приложни приноси

Основните научни приноси на дисертацията са следните:

- Въведени са новите теоретични техники: coupling, координатна декомпозиция, степен на наследяване и разширена апроксимираща линейна таблица по координати (CELAT), с чиято помощ задачата за оптимизиране на нелинейността на С-кутии се свежда до и решава с помощта на SAT алгоритъм.
- Предложена е нова техника за визуализация на аномалии в С-кутиите, която показва, че значителна част от тях имат скрити структури и са следователно уязвими.
- Чрез доказано разлагане на множеството от събираеми е реализиран алгоритъм за оптимизиране на качествения фактор, намаляващ изискването за памет с един порядък, без това да влияе на скоростта.
- Предложен е нов алгоритъм, който чрез евристичен shotgun hill climbing подход дава възможност да се намират двоични последователности с малки PSL стойности.
- Дефиниран е нов клас от крайни двоични последователности с четна дължина, наречени косо-симетрични.

Научно-приложните приноси са:

- Конструирани са биективни 8x8 C-кутии за които и 8-те координати имат максимална стойност на нелинейност 116.
- Използвайки алгоритъма за псевдослучайна генерация на косо-симетрични последователности са намерени такива с MF стойности по-големи от 5 (за дължини до $10^5+1$). Това оборва хипотеза на Bernasconi, според която стохастична процедура на търсене не може да доведе до MF повече от 5 за последователности с дължина над 200.
- Намерени са двоични последователности с дължини между 106 и 300, които имат рекордни стойности на PSL.
- Имплементиран е паралеризируем алгоритъм за намиране на минимално PSL сред двоична последователност и нейните ротации като са обследвани всички $m$-последователности с дължина $2^n-1, n \in \{18,19,20\}$.
- Намерени са всички PSL-оптимални Лежандрови последователности до дължина 432100 и е изказана хипотезата, че броят на всички такива последователности при $N > 235723$ е строго ограничен отдолу от $\sqrt{N}$.

Признавам посочените в дисертацията научни и научно-приложни приноси.

**6. Публикации и участия в научни форуми**

В списъка с публикации по дисертацията има 9 статии, като значителна част от тях са публикувани в реномирани научни издания, включени в първи квартил (Q1) на световните бази WOS и Scopus. Точно половината от публикуваните статии с импакт-фактор са самостоятелни, а другите 3 са в съавторство с научния ръководител проф. Цонка Байчева и с д-р Николай Николов.

Две от статиите все още не са публикувани, но са представени пред научната общност в Arxiv, а една е включена в сборник от научна конференция. Три от статиите са в IEEE Access, което представлява научен журнал в топ 85% (по Scopus) в направлението "компютърни науки" и има импакт-фактор 3.476. Две статии са публикувани в IEEE Signal Processing Letters с импакт-фактор 3.109, намиращ се в топ 90% на категорията приложна математика. Една статия е в журнала IEEE Communications Letters имащ IF 3.436 отново в категория компютърни науки. Считам, че участието на дисертанта във всички съвместни публикации е равностойно на останалите съавтори. Броят на статиите значително надвишава изискванията на ППЗРАСРБ.

**7. Мнения, забележки и препоръки**

Една дисертация за ОНС „доктор", както беше казано и на предварителното обсъждане, не представлява просто сбор от статии. В тази връзка, намирам за

странно фактът, че в уводните части на съответните глави (секции) няма цитирания към публикациите на дисертанта, от които съответно се състоят тези глави (секции). Такива цитирания има единствено в края на секциите от глава 4. Нещо повече, на определени места се препраща читателя към статиите на дисертанта, които вече са намерили място в дисертацията (дори са самата ѝ същност) и логично би било да се цитират съответните глави (секции) от труда. Именно това би трябвало да представлява дисертацията – цялостен, кохерентен труд.

**8. Заключение**

По мое мнение, представеният дисертационен труд „Конструиране на булеви функции и цифрови последователности за криптологията и комуникациите“ с автор Мирослав Маринов Димитров съдържа научни и научни-приложни резултати, които представляват оригинален принос в криптографията, информатиката и защитата на данни. Дисертантът очевидно има задълбочени теоретични знания в областта на С-кутиите и двоичните последователности, както и способност за самостоятелна научна работа. С това считам, че той отговаря напълно на изискванията установени от ЗРАСБ, както и на правилниците на БАН и на ИМИ, така че, в резултат на тази рецензия, с убеденост предлагам на уважаемото научно жури да гласува **ДА СЕ ПРИДОБИЕ** образователната и научна степен „доктор” от Мирослав Маринов Димитров в професионално направление 4.6. „Информатика и компютърни науки“.

Член на журито……..

/проф. дмн Николай Янков/

05.01.2023 г.
Шумен