СТАНОВИЩЕ

на дисертационен труд за придобиване на научна степен "доктор" в

област на висше образование: 4. „Природни науки, математика и информатика”,
професионално направление: 4.6 „Информатика и компютърни науки”,
научна специалност: 01.01.12 Информатика.

Автор: Мирослав Маринов Димитров, докторант в секция „Математически основи на информатиката“, ИМИ - БАН

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

Становището е изготвено от доц. д-р Златко Георгиев Върбанов, ВТУ „Св.св. Кирил и Методий“, в качеството ми на член на научното жури, съгласно заповед №521/2.12.2022 г. на Директора на Института по математика и информатика към БАН.

1. Обща характеристика на дисертационния труд и представените материали

В дисертацията са разработени методи за конструиране на булеви функции, С-кутии и различни видове цифрови последователности, приложими в криптологията и съвременните комуникации. С-кутии, генерирани чрез помощта на функции от теорията на хаоса са детайлно анализирани, с цел измерване тяхната устойчивост към линейния криптоанализ. Голяма част от публикуваните трудове, свързани с теорията на хаоса, разглеждат само средната стойност на нелинейността на координатите на дадената С-кутия, игнорирайки останалите компоненти. Предложените два евристични алгоритъма, които стартират от напълно случайно генерирана С-кутия, достигат рекордни средни стойности на нелинейност, изчислена само върху координатите на С-кутията. Също така е предложен ефикасен алгоритъм за конструиране на двоични редици, с помощта на който в дисертационния труд са достигнати рекордни PSL стойности на двоични редици с дължини между 106 и 300. Предложен е и алгоритъм за успешно достигане на MF (Merit Factor) стойности над 5 за двоични редици с дължини до сто хиляди.

Дисертационният труд (в представения вариант на английски език) съдържа общо 190 страници. Състои се от увод, четири глави, заключение, авторска

справка, литература, списък с публикации по дисертацията и две приложения A и B (обемът на приложенията е 55 страници).

2. Данни за кандидата

Мирослав Димитров е завършил бакалавърска степен „Информатика“ през 2009 г. и магистърска степен „Защита на информацията в компютърните системи и мрежи“, и двете в Софийски университет. Започва да работи в ДАНС през пролетта на 2017 г. През същата година записва обучение в докторантура към ИМИ-БАН.

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

Уводът (отбелязан като Глава 1) съдържа представяне на проблемите, които се решават в дисертационния труд, както и описание на съдържанието на следващите глави. Глава 2 съдържа теоретичните основи на разработката и предварителни резултати. Тук са включени дефинициите и означенията, използвани по-нататък в работата. Раздел 2.3 в тази глава съдържа анализ на някои популярни C-кутии (S-boxes), като в следващия раздел е показано как те могат да бъдат разделени на 4 различни типа. В последния раздел на тази глава проблемът, свързан с нелинейната оптимизация на C-кутиите е представен като проблем за удовлетворимост.

Глава 3 е посветена на реверсивното инженерство на C-кутии. В нея се разглежда стратегия за намиране на аномалии в структурите на C-кутиите, чрез използването на спектрален анализ, разширявайки стратегията, представена от Perrin в дисертацията му „Cryptanalysis, reverse-engineering and design of symmetric cryptographic algorithms“ от 2017 г.

Глава 4 е цялостно ориентирана към PSL (peak sidelobe level) проблема. PSL е критерий за намирането на двоични редици с колективно малки апериодични автокорелационни характеристики. От практическа гледна точка, най-желаното свойство на дадена двоична редица е наличието на нисък PSL. В Раздел 4.1 е предложен ефикасен алгоритъм за конструиране на двоични редици, с помощта на който са достигнати рекордни PSL стойности на двоични редици с дължини между 106 и 300. В Раздел 4.2 е предложен друг алгоритъм, чиято линейна сложност позволява намирането на рекордни PSL стойности, приложим и за редици с по-голяма дължина. В Раздел 4.3 се разглеждат различни параметри, заложени в оценъчната функция на алгоритмите от предните раздели. Описани

са и хибридни алгоритми, които използват някои добре познати алгебрични конструкции. В края на главата се разглежда един известен изчислителен проблем за намирането на най-ниската PSL стойност измежду дадена редица и всички възможни нейни ротации.

В последната глава се разглежда Merit Factor (MF) проблема. MF е друг критерий за намирането на двоични редици с колективно малки апериодични автокорелационни характеристики. Разглеждат се няколко полезни математически свойства, които описват връзката между дадена косо-симетрична двоична редица и получената от нея редица посредством промяната на точно 2 елемента. Изведените свойства, позволяват изискуемата памет за съществуващите алгоритми да бъде редуцирана от n^2 до n. Предложеният алгоритъм успешно достига MF стойности над 5 за двоични редици с дължини до $10^5 + 1$.

4. Апробация на резултатите

Дисертацията е написана въз основа на 9 труда. Те са публикувани или приети за публикуване както следва:

- 6 в международни списания с импакт фактор и квартил Q2;
- 1 в рецензирани сборници на международни конференции;
- 2 под печат (публикувани в arxiv.org)

Шестте публикации с импакт фактор и квартил Q2 са напълно достатъчни за изпълнението на минималните национални изисквания на ЗРАСРБ (те дават на кандидата общо 6 x 60 = 360 точки, а публикацията в сборника на 2020 International Conference on Information Technologies носи още 18 точки). Като цяло, представените научни трудове категорично покриват и многократно надвишават минималните национални изисквания и съответно допълнителните изисквания на ИМИ при БАН за придобиване на образователна и научна степен „доктор“ в научната област и професионално направление на процедурата.

5. Отражение на резултатите на дисертацията в трудове на други автори

Представен е списък с общо 45 цитирания на 8 от трудовете на кандидата. Почти половината от тях са на публикацията „On the design of chaos-based S-boxes“ (общо 22 на брой). Друга много цитирана публикация е „Efficient generation of low autocorrelation binary sequences” (с 11 цитирания).

6. Оценка на приноса на кандидата в съвместните публикации

Пет от публикациите по дисертацията са самостоятелни, три са написани в съавторство с научния ръководител на докторанта и още един съавтор, една е с други трима съавтори. От приложените документи е видно, че приносът на кандидата в съвместните публикации е безспорен и може да се счита, че е равностоен с този на другите съавтори.

7. Автореферат и справка за приносите

Написани са достатъчно подробно и дават ясна и адекватна представа за съдържанието и основните резултати на дисертацията.

8. 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, 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 при БАН за придобиване от кандидата на образователната и научна степен „доктор“ в научната област 4. Природни науки, математика и информатика и 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 конкурса научни трудове. Въз основа на гореизложеното, препоръчвам на научното жури да присъди на Мирослав Маринов Димитров **да бъде присъдена научната степен „доктор”** в професионално направление 4.6. Информатика и компютърни науки.

12.01.2023 г. Подпис:

/доц. д-р Зл. Върбанов/