# Р Е Ц Е Н З И Я

на дисертационен труд
за придобиване на образователната и научна степен "Доктор"

**Област: 4. "Природни науки, математика и информатика"**

**Научно направление: 4.6. "Информатика и компютърни науки"**

**Тема: "Designing Boolean Functions and Digital Sequences for Cryptology and Communications"**

**Автор: Мирослав Маринов Димитров**

**Тема на дисертационния труд**

Основната задача, която се изследва в настоящия дисертационен труд е конструиране и анализ на булеви функции, S-кутии и цифрови редици. Така този труд може да бъде отнесен към криптографията като задачите, които се решават в него носят комбинаторен характер. Тези задачи добиха изключителна популярност в последните няколко десетилетия, която се свързва с нарасналата нужда от защита на данните и по-специално с конструирането на надеждни блокови шифри.

Резултатите в този труд имат отношение най-вече към симетричната криптография. Всеки блоков шифър има нелинейна част, наречена S-кутия която гарантира устойчивост към известните криптографски атаки. Този модул трябва да бъде много внимателно проектиран и да отговаря на строги математически критерии. Това е и мотивацията зад този труд.

Работата систематизира и обобщава изследванията на автора през последните няколко години.

**Литературен обзор**

Общото ми впечатление е, че дисертантът познава отлично съвременното състояние на разглежданите проблеми. Голяма част от изследванията му са върху кръг от задачи и хипотези от симетричната криптография, считани за значими в теоретичен план. Докторантът демонстрира задълбочено познаване на областта на изследванията и възможности творчески да прилага знанията си.

**Методика**

В изследванията си докторантът използва широк арсенал от средства. Резултатите от дисертационния труд са получени не само чрез нестандартни компютърни програми, разработени от докторанта, но част от твърденията са доказани и с математически доказателства, използващи идеи от дискретната математика, целочисленото оптимиране и комбинаториката.

**Съдържание и резултати на дисертационния труд**

Дисертационният труд е в обем от 190 нестандартни машинописни страници и се състои от увод, пет глави, списък на използваната литература, включващ 152 заглавия и две приложения.

По-долу ще изложа накратко съдържанието на отделните глави от дисертацията.

Глава 1 служи за въведение в проблематиката на дисертационния труд. Тя започва с мотивация за значимостта на S-кутиите и необходимостта от силни S-кутии, за гарантиране на устойчивост срещу различни видове криптанализ – линеен, диференциален, алгебричен. Подчертана е значимостта на редица чисто математически задачи за решаване на този проблем като конструирането на редици с ниска извънфазова автокорелация. Разгледани са различни класически характеристики, свързани с редици като peak sidelobe level и merit factor. Формулирани са някои интересни задачи, които са нерешени към настоящия момент като намирането на оптималните стойности на PSL за редици с дължина 84, минимизиране на merit factor-а. Тук е формулирана и основната задача на дисертационния труд – изследване на стратегии за конструиране и анализ на булеви функции. По-нататък е изложено накратко и съдържанието на дисертационния труд.

Оригиналните приноси на автора се съдържат в глави 2, 3, 4 и 5.

В Глава 2 са изложени някои прдварителни сведения за булеви функции. Въведени са различни нормални форми за булеви функции, дефинирани са трансформациите на Уолш-Ададмар, въведени са векторни булеви функции, S-кутии и свързаните с тях обекти. Анализиран е богат набор от S-кутии и е направена класификация на стратегиите за конструиране на $S$-кутии. Разгледана е задачата оптимизация на $S$-кутия като задача на целочисленото оптимиране. Предложена е програма, която оптимизира нелинейността на зададена $S$-кутия с минимален брой промени. Това свойство е полезно, защото оптимизационната програма може да се фокусира върху слабите компоненти на една $S$-кутия без да разваля останалите. Ефективността на предложения алгоритъм е демонстрирана чрез прилагането му върху $S$-кутиите на два си-

метрични шифъра – Skipjack и Кузнечик. Показано е и съществуването на $S$-кутия със средна покоординатна нелинейност 116, докато опитите да се конструира такава със средна нелинейностт 118 са се оказали неуспешни.

В Глава 3 се разглеждат различни стратегии за откриване на скрити мотиви и аномалии в популярни S-кутии. С това може не само да се докаже, че изследваните кутии не се получени чрез псевдо-случайно генериране, но и да се получат допълнителни сведения за вътрешната структура на S-кутиите. Това дава възможност за т.нар. ривърз енджинийринг – пълно разкриване на скритата структура на кутията.

Глава 4 е посветена на задачата за получаване на редици с ниска автокорелация или, по-конкретно, оптимизация на PSL (peak sidelobe level), което се дефинира максималната стойност на модула на автокорелацията $|C_u(B)|$, взето по всички отмествания $u$. В раздел 4.1 е представен ефективен евристичен алгоритъм, основан на т.нар. shotgun hill-climbing. Алгоритъмът започва работа от случайна двоична редица с дължина $n$ като получава за вход и някаква таргет-стойност за PSL, означена с $G$. При достигане на $G$ алгоритъмът прекратява работа; в противен случай преминава към някаква съседна (по Хеминг) редица. Ако всички съседни редици не подобряват стойността на текущия PSL се прави скок като броят на допустимите скокове е ограничен от някаква константа. Този алгоритъм е приложен за генериране на двоични редици с дължини между 106 и 300 като в повече от половината случаи са получени подобрения на известните до момента оптимални стойности. В следващия раздел е предложен метод за генериране на дълги двоични редици с ниска стойност на PSL. Сложността на получения алгоритъм по време и по памет е линейна (от дължината на редицата). Направени са експерименти, при които са получени няколко редици с рекордни PSL стойности. В следващия раздел са представени и редица хибридни алгоритми за получаване на двоични редици с ниска автокорелация.

В глава 5 се разглежда задачата за оптимизиране на т.нар. merit factor, дефиниран като

$$MF(B) = \frac{C_0(B)}{2\sum_{u=1}^{n-1} |C_u(B)|^2}.$$

Конструирани са нови класове от двоични редици с висок MF. Авторът ограничава изследването върху класа на т. нар. кососиметрични двоични редици, въведени от Голей. Конструирани са дълги редици ($n > 200$) които надхвърлят стойностите за $MF$ предсказани в хипотезата на Бернаскони. Описан е алгоритъм за намиране на двоични редици с висока стойност за merit factor-а.

**Приноси на дисертационния труд**

По мое мнение по-важните приноси в дисертационния труд се свеждат до следното:

(1) Направен е анализ на голям брой $S$-кутии и е установено, че т.нар. $S$-кутии, основани на теория на хаоса са податливи на линеен криптанализ.

(2) Доказано е съществуването на $8 \times 8$ биективни $S$-кутии с максимална нелинейност 116 по всички координати

(3) Предложена е стратегия за откриване на скрити регулярности и ривърз енджинийринг чрез използване спектрография на $S$-кутии.

(4) Предложен е ефективен евристичен алгоритъм за конструиране на двоични редици с нисък $PSL$. Конструирани са редици с дължини между 106 и 300 с рекордни $PSL$ стойности.

(5) Конструирани са нови класове от двоични редици с висок MF.

(6) Построен е нов клас от крайни двоични редици с четна дължина с алтернираща ащтокорелационни стойности равни по модул на 1.

(7) Представен е алгоритъм за генериране на дълги двоични редици с висок merit factor.

**Забележки и коментари по дисертационния труд**

Във връзка с дисертационния труд имам следните въпроси, забележки и коментари:

(1) В дефиниция 2.2.2 биективни S-кутии са възможни само когато $m = n$.

(2) Във формулата за $MF(B)$ на стр. 48: какъв е смисълът от двойката в знаменателя и не е ли винаги $C_0$ равно на дължината на редицата?

(3) Въобще какъв е смисълът от т.нар. merit factor? Не е ли все едно да минимизираме сумата от квадратите на $C_u$.

(4) Дефиниция 2.2.7: Какво наричаме дължина на линейна функция?

(5) Дефиниции 2.2.7 и 2.2.8 са неясни.

(6) Би било добре текстът да съдържа дефиниция на понятието нелинейност на двоична функция, не само нелинейност на $S$-кутия.

**Публикации по дисертационния труд**

Резултатите от дисертационния труд са публикувани в 9 статии, седем от които са излезли от печат, а две са депозирани в arXiv. Списанията, в които са отпечатени тези работи са следните:

- IEEE Access – 3 статии;

- IEEE Signal Processing Letters – 2 статии;

- IEEE Communication Letters – 1

- Proceedings of the International Conference on Information Technologies (InfoTech) – 1 статия;

- arXiv – 2 statii

Шест от статиите са с импакт-фактор, надхвърлящ 3, като и шестте са в Q2, една е в сборник с доклади от научна конференция, а две са депозирани в arXiv. В пет от представените статии докторантът е единствен автор, три са с двама, а една – с трима съавтори.

Публикационната активност на Мирослав Димитров е изключително впечатляваща. Тя включва голям брой публикации, излезли в рамките само на три години и то в много престижни издания, всички от които са в Q2. Това говори за високо ниво на провежданите изследвания. Представените публикации не само удовлетворяват, но и далеч надхвърлят минималните национални изисквания за присъждане на образователната и научна степен "доктор".

**Авторство на получените резултати**

В голяма част от публикациите докторантът е единствен автор. Тъй като познавам научните интереси на докторанта и следя работата му в последните години, за мен няма съмнение, че приносът му в съвместните публикации е поне равностоен на този на останалите автори. Публикациите удовлетворяват минималните изисквания в Закона за развитие на академичния състав в Република България, Правилника за прилагането му и Правилника на Института по математика и информатика.

**Цитирания на публикациите от дисертационния труд**

Докторантът е приложил списък от 48 цитирания на свои публикации. Макар работите му да са излезли от печат сравнително неотдавна те вече са привлекли вниманието на работещоте в областта на симетричната криптография. Това показва, че изследванията му са получили висока оценка от специалистите в тази област. За мен няма съмнение, че този списък ще бъде продължен в съвсем близко бъдеще.

**Автореферат и авторска справка**

Авторефератът и авторската справка са направени съгласно изискванията и отразяват правилно резултатите и приносите в дисертационния труд.

**Заключение**

Считам, че представеният дисертационен труд **"Designing Boolean Functions and Digital Sequences for Cryptography and Communications"** (Конструиране на булеви функции и цифрови редици за криптографията и комуникациите) с автор **Мирослав Маринов Димитров** съдържа интересни резултати, които представляват оригинален принос в асиметричната криптография и теория на булевите функции. Докторантът показва изключително задълбочени теоретични познания в тези области и с това отговаря на изискванията на Закона за развитие на академичния състав в Република България, Правилника за неговото прилагането и Правилника на Института по математика и информатика за присъждане на образователната и научна степен "Доктор". В дисертационния труд и свързаните с него публикации няма установено плагиатство.

Изложеното по-горе ми дава основание да дам **положителна оценка** на представения дисертационен труд и да препоръчам на Уважаемото Жури да присъди на Мирослав Маринов Димитров образователната и научна степен "Доктор"в област 4. "Природни науки, математика и информатика", научно направление 4.6 "Информатика и компютърни науки".

София, 12.01.2023 г. Рецензент:

(проф. д.м.н. Иван Ланджев)