# Р Е Ц Е Н З И Я

на дисертация

за придобиване на образователната и научна степен „доктор“

**Област на висше образование:** 4. Природни науки, математика и информатика

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

**Автор:** Мирослав Цветков Марков

**Тема:** ЕФЕКТИВНИ АЛГОРИТМИ С ПРИЛОЖЕНИЕ В КРИПТОГРАФИЯТА С ПУБЛИЧЕН КЛЮЧ И ТЕОРИЯ НА КОДИРАНЕТО

**Рецензент:** Проф. дмн Илия Георгиев Буюклиев
Секция „Математически основи на информатиката”,
Институт по математика и информатика при БАН

На основание Заповед №208/18.07.2024 на Директора на ИМИ-БАН за разкриване на процедура за защита на дисертационен труд на докторант Мирослав Цветков Марков съм утвърден за член на Научното жури по процедурата. Тази рецензия е изготвена и представена на основание Решение на Научното жури (Протокол №1/24.07.2024) за разпределение на дейностите между членовете на Научното жури по процедурата. Настоящата рецензия е изготвена в съответствие с изискванията на Закона за развитие на академичния състав в Република България (ЗРАСРБ), Правилника за неговото приложение (ППЗРАСРБ), и Правилника за условията и реда за придобиване на научни степени и заемане на академични длъжности в Института по математика и информатика при БАН. Предоставени са ми всички необходими документи, включително заявление до Директора на ИМИ при БАН за допускане до защита, професионална автобиография, заповед за зачисляване в докторантура, протоколи за издържаните изпити съгласно плана на докторантурата, заповед за отчисляване от докторантура, заповед на Директора на ИМИ за обсъждане на дисертационния труд от първично звено, протокол от обсъждане на дисертационния труд от първичното звено, списък на публикациите по дисертацията, списък на цитиранията на публикациите по дисертацията, копия от публикациите по

дисертацията, дисертационен труд, справка за приносите в дисертацията, публикациите по темата на дисертацията и автореферат.

## 1. Кратки биографични данни за дисертанта.

Мирослав Марков е завършил магистратура по електроника и автоматика в Технически университет, София, през 1996 г., има и бакалавърска степен по математика и информатика от СУ „Св. Климент Охридски“ от 2006 г. От 1992 до 2008 година ръководи екипи за създаване на софтуер за нуждите на МВР. След това продължава като главен експерт в същата област към ДАНС. От август 2022 година работи като математик в секция МОИ на ИМИ при БАН. От 2019 година е зачислен в редовна докторантура към ИМИ. Оттогава той активно се включва в научните форуми, организирани от секцията и института. От автобиографията, която е представил, става ясно за много допълнителни курсове и специализации, отнасящи се до компютърни системи и архитектури, операционни системи и езици за програмиране.

## 2. Актуалност на тематиката.

Дисертационният труд на Мирослав Марков е посветен на изследвания в областта на криптографията и алгебричната теория на кодирането, и е свързан с две конкретни задачи. Първата се отнася до намиране броя на точките върху елиптична крива, а втората е за намиране на тегловното разпределение на код на Рид-Малер с параметри RM(4,9).

Важността и актуалността на първата задача се определя от факта, че елиптичните криви намират все по-голямо приложение в много области на математиката и особено на криптографията. Като пример можем да посочим алгоритъма ECDSA за цифров подпис, базиран на елиптична крива. Основен аспект при проектирането на една криптосистема, базирана на елиптични криви, е намирането на броя на точките върху избраната крива, тъй като той играе централна роля при определяне на сигурността, размера на ключа и производителността на криптографската система.

Изследването на тегловни инварианти като радиус на покритие и теглово разпределение на кодовете на Рид-Малер е пряко свързано с изучаването на криптографските свойства на булевите функции и вектор-булевите функции, а вектор-булевите функции са основния нелинеен компонент на всеки блоков шифър. Мога да определя тази задача като особено важна за работата, защото тя освен че е интересна и актуална, се намира на границата на възможното за решаване с наличния теоретичен и изчислителен ресурс.

## 3. Обща характеристика на дисертационния труд.

Дисертацията е в обем от 74 страници и се състои от увод, три глави, две приложения и литература, включваща 59 заглавия. В увода е представена мотивация и исторически бележки за разглежданите задачи. Първа и втора глава се отнасят до елиптични криви. Трета глава е посветена на пресмятането на тегловото разпределение на кодовете на Рид-Малер RM(4,9). Поради това, че предварителните понятия и твърдения за двете задачи са различни, авторът започва всяка глава с въведение, в което представя необходимата известна фактология.

Глава 1 е посветена на изследванията на дисертанта върху елиптичните криви от вида $y^2 = x^3 + a \ (mod\ p), a \neq 0$. Първата част е представя въведение в задачата, изброяване на някои от използваните подходи, както и информация за тяхната сложност. Във втора част са дадени необходимите дефиниции и предварителни твърдения. След това са представени разработеният метод и използваните алгоритми. Главата завършва с примери за използване на алгоритмите върху специфични елиптични криви и оценка на сложността. Тази глава следва публикациите на дисертанта с неговия научен ръководител „An Efficient Approach to Point-Counting on Elliptic Curves from a Prominent Family over the Prime Field $\mathbb{F}_p$“ в списание *Mathematics* и „An Approach for Computing the Number of Points on Elliptic Curve $y^2 = x^3 + a \ (mod\ p)$ via Explicit Formula for That Number Modulo *p*“ in: *Ninth International Workshop on Signal Design and its Applications in Communications* (IWSDA) (2019).

В следващата глава се изследва семейството от елиптични криви $\mathcal{D}_p$ от вида:

$$\mathcal{D}_p = \{D_a : y^2 = x^3 + ax \ (mod\ p), a \neq 0\}.$$

Целта е да се опише общ подход за определяне на реда (броя на точките) на крива от това семейство в зависимост от $a$ и $p$. Изчислителните аспекти на преброяването на точките на криви от това семейство са представени в трета част. След пресмятане на сложността дисертантът заключава, че предложеният подход подобрява значително най-доброто известно досега решение. Резултатите са публикувани в „Point-Counting on Elliptic Curves Belonging to One Prominent Family“, *Algebraic and Combinatorial Coding Theory* (ACCT) (2020).

Трета глава е посветена на намиране на спектъра на кода на Рид-Малер RM (4,9). За решаването на задачата за теглови спектър на произволен линеен код има няколко подхода, свързани с пълно изчерпване, бързи трансформации и други. Но параметрите на кода, особено размерността 256, в разглеждания случай правят немислимо

използването на общи алгоритми. Затова от решаващо значение е използването на структурата и много от свойствата на кодовете на Рид-Малер, базирани на връзката им с булевите функции. Общи подходи при решаване на задачи с голяма изчислителна сложност е използването на теоретични решения или редуциране на изчисленията с теоретични разсъждения.

Броят на някои от теглата се получава на базата на твърдение на Gleason за спектрите на самодуалните двоични двойночетни кодове, към който клас принадлежи и разглежданият код. Това се оказва недостатъчно за окончателно решаване на задачата. На следваща стъпка се използва подход, в основата на който стои метод на Sarwate.

Стратегията описана в дисертацията се базира на следните факти:

- Код на Рид-Малер от по-висок ред може да се разглежда като получен от код на Рид-Малер от по-нисък ред с рекурентна формула или $(u, u+v)$ конструкция.
- Разглеждане на линейна и афинна еквивалентност на съседни класове на код на Рид-Малер от ред $r$, които се съдържат в код на Рид-Малер от ред $r+1$ и $r+2$.
- Фактът, че афинно еквивалентните съседни класове имат едни и същи разпределения.
- Използване на известната теория за връзката между спектъра на код на Рид-Малер от ред $r$ и спектрите на съседните класове по кодове на Рид-Малер от по-нисък ред.

В дисертацията освен подробното описание на теоретичния подход е представен и псевдо код на използваните алгоритми. Изчислителните предизвикателства са решени с използването на нетривиални идеи, сериозни алгоритмични умения, капацитет за използване на ефективни софтуерни пакети и многопроцесорни изчислителни системи. В една от частите в края на главата има подробна оценка на необходимите изчислителни ресурси и използваната налична техника. Това е много показателно за задачи от този тип, защото оптимизация на алгоритмите се прави дотогава, докато необходимият ресурс е не повече от наличния (при разумно време за изчисления).

Дисертацията е добре балансирана като съдържание и следва статиите, публикувани по време на докторантурата. Текстът е добре оформен и показва задълбочено владеене на математическата терминология и умело боравене с изчислителните ресурси. Всяка глава започва с уводна част и завършва със заключение. Това улеснява читателя и му дава възможност да проследи изследването, без да се консултира с други източници.

## 4. Приноси и значимост на разработката.

Приемам и одобрявам представените приноси, посочени от Мирослав Марков. Бих откроил следните от тях:

- По отношение на елиптичните криви: Разработени са ефективни методи за пресмятане на реда на елиптична крива и са изведени явни формули за този ред за криви от следните две семейства:

$$\mathcal{E}_p = \{E_a: y^2 = x^3 + a \ (mod\ p), a \neq 0\},$$

$$\mathcal{D}_p = \{D_a: y^2 = x^3 + ax \ (mod\ p), a \neq 0\}.$$

  Разработен е ефективен метод за едновременно пресмятане на шестте възможни реда, свързани със семейството $\mathcal{E}_p$, при фиксирано p ≡ 1 (mod 6), както и на четирите възможни реда, свързани със семейството $\mathcal{D}_p$, при фиксирано $p \equiv 1\ (mod\ 4)$. Сложността на този метод е $\tilde{O}(log^2 p)$.

- По отношение на пресмятане на тегловия спектър на кода RM (4,9):

– Разработен е ефективен алгоритъм за пресмятане на тегловото разпределение на двоичния код на Рид-Малер RM(4, 9), като е комбиниран подхода на Sarwate с резултатите за класификацията на Булевите функции според афинната им еквивалентност, публикувани през 2008 и 2023 г.

– Пресметнато е тегловото разпределение на двоичния код на Рид-Малер RM (4,9), който има параметри [512,256,32] (дължина 512, размерност 256 и минимално разстояние 32).

## 5. Публикации по дисертационния труд и цитирания.

Дисертацията на Мирослав Марков се основава на изследователска работа, описана в четири публикации, от които една статия в научно списание и три в сборници от международни научни конференции. Всички статии са на английски език. Резултатите, свързани с елиптичните криви от фамилията $\mathcal{E}_p$, са публикувани в списание *Mathematics*, което има JCR-IF от Web of Science и попада в квартил Q1. Тя му носи 75 точки в таблицата с наукометричните показатели. Всичките четири публикации са в съавторство с научния му ръководител доц. Юри Борисов. Считам, че приносът на Мирослав Марков в съвместните публикации е съществен.

Резултатите от този дисертационен труд са докладвани на седем конференции и семинари у нас и в чужбина:

- семинарът *Ninth International Workshop on Signal Design and its Applications in Communications* (IWSDA), проведен в Китай през 2019 година;
- международния семинар по алгебрична и комбинаторна теория на кодирането ACCT‘2020, проведен онлайн;
- конференцията *High-Performance Computing for Mathematics and Applications*, проведена в София през юни 2023 г.;
- тринадесетия международен семинар WCC, проведен в Перуджа, Италия, през юни 2024 г.;
- националните семинари по теория на кодирането през 2019, 2022 и 2023 година.

Дисертантът е представил списък с пет цитирания, от които две са за работите му, посветени на елиптичните криви, и три по отношение на кода на Рид-Малер.

## 6. Автореферат.

Авторефератът правилно отразява съдържанието на дисертационния труд. Бих казал, че оформлението му е малко различно от стандартното. В началото е представена обща характеристика на дисертационния труд, следвана от цели и задачи, методология на изследването, апробация на резултатите и списък на публикациите по дисертацията. След това започва представяне на отделните глави, съответно в 12, 6 и 18 страници. Авторефератът завършва с авторска справка, благодарности и списък с използвана литература. Дисертантът се е опитал да представи доста пълно дисертацията си в него, но според мен би било по-добре първа и трета глава да бъдат описани по-кратко, с акцент върху приносите на автора.

## 7. Лични впечатления.

Познавам Мирослав Марков от неговото зачисляване в докторантура, което беше обсъдено на ежегодния семинар по теория на кодирането през 2018 г. Оттогава насам той е участвал във всички издания на семинара. Там сме дискутирали различни теми, свързани с алгоритми, оптимизация на софтуер, прилагане на високопроизводителни изчисления и използване на суперкомпютър. Впечатленията ми са, че Мирослав Марков е много добре запознат както с нужните му математически теории, така и с разработването на алгоритми, програмирането и използването на високопроизводителни изчислителни технологии.

## 8. Заключение.

Представеният дисертационен труд заедно с приложените научни трудове удовлетворява всички изисквания на Закона за развитие на академичния състав в Република България (ЗРАСРБ), Правилника за неговото приложение (ППЗРАСРБ), Правилника за условията и реда за придобиване на научни степени и заемане на академични длъжности в БАН и Правилника за условията и реда за придобиване на научни степени и заемане на академични длъжности в ИМИ за придобиване на образователна и научна степен „доктор“ в професионално направление 4.6. Информатика и компютърни науки. Постигнатите резултати ми дават основание да препоръчвам на Уважаемото научно жури да присъди на **Мирослав Цветков Марков** образователната и научна степен „Доктор” в

Област на висше образование: 4. Природни науки, математика и информатика,

Професионално направление: 4.6. Информатика и компютърни науки.

05.09.2024 г. Рецензент:

/проф. дмн Илия Буюклиев/