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”,

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

Тема: ”Ефективни алгоритми с приложение в криптографията с публичен ключ и теория на кодирането”

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 №208/18.07.2024 г. на Директора на Института по математика и информатика към БАН и решение на научното жури Протокол 1/24.07.2024 г.

1. Обща характеристика на дисертационния труд и представените материали

В дисертацията са разработени и представени ефективни алгоритми за определяне на броя на точките върху елиптични криви над просто поле (разглеждат се две конкретни семейства елиптични криви) и за изчисляване на спектъра (тегловото разпределение) на двоичния код на Рид-Малер $R(4,9)$. За всеки от алгоритмите, представени в Глави 1 и 2, е направено сравнение на ефективността, от което се вижда, че тези алгоритми подобряват значително ефективността на известните досега алгоритми. В Глава 3 е извършено изчисляване на тегловото разпределение на двоичния код на Рид-Малер $R(4,9)$, като първо е демонстриран опит чрез теоремата на Gleason и е показано, че по този начин има немалко проблеми и затруднения, затова в следващия раздел е използван методът на Sarwate, чрез който вече се постига желания резултат. Приложение А съдържа таблици, в които е описано тегловото разпределение.

Дисертационният труд (в представения вариант) съдържа общо 74 страници. Състои се от увод, три глави, заключение, авторска справка, литература (цитирани са общо 59 източника), списък с публикации по дисертацията и две приложения А и Б (обемът на приложенията е 6 страници).

2. Данни за кандидата

Мирослав Марков е завършил магистърска степен „Съобщителна и осигурителна техника и системи“ през 1996 г. в ТУ-София и допълнително бакалавърска степен „Математика и информатика“ през 2006 г. в Софийски университет. От април 1992 г. до март 2008 г. работи в различни структури на МВР. Започва работа в ДАНС през пролетта на 2008 г. От август 2022 г. работи в 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 съдържа представяне на проблемите, които се решават в дисертационния труд, както и описание на съдържанието на следващите глави. В началото на всяка от главите са представени теоретичните основи на разработката и предварителни резултати. Глава 1 е посветена на разработването на ефективен детерминистичен алгоритъм за пресмятане на реда (броя на точките) на семейството от елиптични криви:

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

След първоначалното представяне (Раздел 1.2) на предварителните знания, в Раздел 1.3 се излага подхода към проблема, включително подобрените оценки за изчислителната сложност при големи стойности на *p*. Раздел 1.4 съдържа примери с прости числа за модул (в единия пример *p* е модулът на елиптичната крива *secp256k1*, а в другия числото *p* е специално конструирано) и също така обсъжда резултатите от експеримент с програма за сравняване производителността на предложената алгоритмична техника спрямо тази на алгоритъма SEA в разглеждания сценарий.

В Глава 2 е представен метод за преброяване на точките върху елиптични криви от вида

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

След въведението и встъпителните бележки, в Раздел 2.3 е описан подхода, използван в разработката. Първо се дава явна формула за реда на елиптичната крива D_a. След това се характеризират по-прецизно възможните редове на криви в съществения случай p ≡ 1 (mod 4). В третата част на този раздел се разглеждат изчислителните аспекти на преброяването на точките в D_p, когато *p* е голямо просто число. В Раздел 2.4 е представен пример с просто число, което се

използва за модул в параметрите на елиптичната крива secp224r1 (спецификация на NIST за 224-битова елиптична крива). Главата завършва с обобщение на резултатите.

Глава 3 е цялостно ориентирана към теория на кодирането и по-специално към изчисляване на спектъра (тегловото разпределение) на двоичния код на Рид-Малер R(4,9). В Раздел 3.1 са представени основните понятия. В Раздел 3.2 е представен опит за намиране на тегловото разпределение чрез теоремата на Gleason и свързаните с това проблеми и затруднения. В Раздел 3.3 чрез метода на Sarwate е извършено пресмятането на тегловото разпределение, оценени са изчислителните разходи и са представени използваните компютърни ресурси. В заключението на тази глава са обобщени резултатите.

4. Апробация на резултатите

Дисертацията е написана въз основа на 4 труда. Те са публикувани или приети за публикуване както следва:

- 1 в международни списания с импакт фактор и квартил Q2;
- 3 в рецензирани сборници на международни конференции;

Публикацията с импакт фактор и квартил Q2 е напълно достатъчна за изпълнението на минималните национални изисквания на ЗРАСРБ (тя дава на кандидата 75 точки, а трите публикации в рецензирани сборници носят още 3x18 = 54 точки). Като цяло, представените научни трудове категорично покриват и 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 5 цитирания на 3 от трудовете на кандидата. Три от цитиранията са на публикацията „Weight Distribution of the Binary Reed-Muller Code R(4, 9)“. Другите две цитирани публикации са „An Approach for Computing the Number of Points on Elliptic Curve $y^2 = x^3+a \pmod p$ via Explicit Formula for That Number Modulo p” и „An Efficient Approach to Point-Counting on Elliptic Curves from a Prominent Family over the Prime Field F_p“ .

6. Оценка на приноса на кандидата в съвместните публикации

Представените публикации са написани в съавторство с научния ръководител на докторанта. 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 Цветков Марков **да бъде присъдена научната степен „доктор”** в професионално направление 4.6. Информатика и компютърни науки.

29.08.2024 г. Подпис:

/доц. д-р Зл. Върбанов/