С Т А Н О В И Щ Е

от проф. дмн Стоян Недков Капралов

Технически университет – Габрово,

относно

дисертационния труд на на Мирослав Цветков Марков

„Ефективни алгоритми с приложение в криптографията

с публичен ключ и теория на кодирането“

представен за придобиване на образователната и научна степен „доктор“

в област на висше образование 4. Природни науки, математика и информатика

професионално направление 4.6. Информатика и компютърни науки

докторска програма Информатика

Настоящото становище е написано на основание Заповед № 208/18.07.2024 г. на Директора на ИМИ БАН и на решение от първото заседание на научното жури по процедурата.

1. **Данни за докторантурата**

Мирослав Марков е зачислен в редовна докторантура в ИМИ на БАН през 2019 г. През 2022 г. е отчислен с право на защита.

На 26.06.2024 г. е проведено предварително обсъждане на представения дисертационен труд.

2. **Структура на дисертацията**

Дисертацията се състои от 12 предварителни страници и 75 страници основен текст.

Предварителните страници съдържат декларация за оригиналност, благодарности, съдържание, списък на таблиците, списък с абревиатури и съкращения.

Основният текст се състои от Резюме, Увод, три глави, Библиография, две приложения, списъци на докладите и публикациите по дисертацията.

3. **Актуалност на изследвания проблем**

Използването на елиптични криви в криптографията е предложено преди около 60 години, като в последните 20 години изследванията и практиката в тази област бележат изключителен разцвет.

Основното предимство на криптографията с използване на елиптични криви, в сравнение с традиционната криптография с публичен ключ е осигуряването на аналогично ниво на защита, но с по-къси ключове.

Броят на точките върху елиптична крива над крайно поле е важен параметър, от който зависи сигурността, размера на ключа и производителността на криптографската система.

Кодовете на Рид-Малер са важен клас кодове в теорията на кодирането, използвани за поправяне на грешки при предаване на информация по канал с шум. Тези кодове са широко използвани в различни приложения, включително в комуникационни системи и космически мисии, където надеждността на предаваната информация е от критично значение.

Дисертацията е посветена на изследвания в две актуални области: 1) определяне броя на точките върху елиптични криви от две семейства; 2) изчисляване тегловото разпределение на двоичния Рид-Малер код R(4,9).

4. Съдържание и приноси на дисертационния труд

В началото на дисертацията е формулирана целта на изследването, както и конкретните задачи, които трябва да бъдат решени.

Глава 1 – "Метод за преброяване на точките върху елиптични криви от вида $y^2 = x^3 + a\ (mod\ p),\ a \neq 0$" се състои от пет раздела. Основни са раздели 1.3 и 1.4.

В раздел 1.3 е представено описание на метода, а в раздел 1.4 са дадени примери.

Глава 2 е посветена на изучаването на елиптични криви от вида $y^2 = x^3 + ax\ (mod\ p),\ a \neq 0$, като структурата на Глава 2 е аналогична на тази от Глава 1.

Изложението в тези две глави демонстрира високата математическа ерудиция на автора, както и неговата експертиза в построяване и анализ на алгоритми.

Приемам научните приноси, относно Глава 1 и Глава 2, формулирани от автора в Авторска справка за приносите в дисертационния труд, а именно получени са явни формули за реда на криви от две семейства. Като научно-приложни приноси в тези глави може да бъде посочено разработването на ефективни алгоритми за едновременно пресмятане на възможните редове, свързани с криви от изследваните семейства.

В Глава 3 с прилагането на многостъпкова стратегия е получен нов резултат – пресметнато е тегловното разпределение на двоичния Рид-Малер код R(4,9). Само описанието на подхода и реализацията на отделните стъпки заема повече от 20 страници.

Заслужава да се отбележи, че изследването се основава на най-нови резултати на други автори, публикувани през 2023 г.

В резултат е получена впечатляващата Таблица А3.

5. Публикации по дисертационния труд

По дисертацията са представени общо 4 публикации. Публикациите са на английски език. Една от публикациите е статия в международно научно списание, а останалите три са доклади на международни конференции. Всички публикации са в съавторство с научния ръководител.

По обем и качество публикациите покриват минималните изисквания за придобиване на образователната и научна степен "доктор".

Някои от резултатите в публикациите предварително са докладвани на национални и международни семинари.

Не са представени данни за забелязани цитирания на публикациите по дисертацията.

6. Авторефератът отразява правилно съдържанието на дисертацията.

7. Забележки по дисертационния труд

Нямам критични бележки.

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, давам своята положителна оценка и потвърждавам, че представения дисертационен труд и научните публикации към него, както и качеството и оргиналността на представените в тях резултати и постижения, отговарят на изискванията на ЗРАС в Република България, Правилника за приложението му и съответните правилници на ИМИ и на БАН за придобиване от кандидата на образователната и научна степен „доктор“ в област на висше образование 4. Природни науки, математика и информатика, професионално направление 4.6 Информатика и компютърни науки. Кандидатът удовлетворява минималните национални изисквания в професионалното направление и не е установено плагиатство в представените по процедурата научни трудове.

Въз основа на гореизложеното, убедено препоръчвам на научното 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.

11.08.2024 г. **Подпис:**

/проф. дмн Стоян Капралов/