Рецензия

по процедура за защита на дисертационен труд на тема:

„ЕФЕКТИВНИ АЛГОРИТМИ С ПРИЛОЖЕНИЕ В КРИПТОГРАФИЯТА С ПУБЛИЧЕН КЛЮЧ И ТЕОРИЯ НА КОДИРАНЕТО“

за придобиване на образователна и научна степен „доктор“

представен от: **Мирослав Цветков Марков,**

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

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

Докторска програма: **„Методи за обработка и защита на данни“,**

секция: **„Математически основи на информатиката“,**

Институт по математика и информатика (ИМИ),

Българска академия на науките (БАН),

Рецензията е изготвена от: **проф., д-р Владимир Тодоров Димитров – Факултет по математика и информатика, Софийски университет „Св. Климент Охридски“**, в качеството ми на член на научното жури, съгласно Заповед № 208 / 18.07.2024 г. на Директора на Института по математика и информатика.

1. **Обща характеристика на дисертационния труд и представените материали**

   За защитата са представени следните материали:

   1. Заявление (молба) до Директора на ИМИ-БАН за допускане до защита, вх. № 468 / 11.07.2024.
   2. Професионална автобиография – европейски формат, 2 страници.
   3. Заповед за зачисляване в докторантура, № 239 / 01.07.2019.
   4. Протоколи за издържаните изпити, съгласно плана на докторантурата, пет протокола за издържани изпити по Excel, Английски език, Блокчейн технологии, Криптология, Сигурност на елиптичната криптография. Всичките изпити са взети с отлична оценка.
   5. Заповед за отчисляване от докторантурата, № 217 / 18.07.2022, с право на защита.

6. Заповед на Директора на ИМИ за обсъждане на дисертационния труд от разширеното научно звено на секция Математически основи на информатиката, № 172 / 10.06.2024.
7. Протокол от обсъждане на дисертационния труд от разширеното научно звено на секция Математически основи на информатиката от 26.06.2024. С решение за допускане до защита.
8. Информационна карта на НАЦИД – образец 1 и образец 3. Регистрация на докторанта с тема на дисертацията и публикации:
    - Borissov, Y. & Markov, M. An Approach for Computing the Number of Points on Elliptic Curve y2 = x^3+a (mod p) via Explicit Formula for That Number Modulo p. In Proceedings of the 2019 Ninth International Workshop on Signal Design and its Applications in Communications, Dongguan, China, 20–24 October 2019, pp. 1–5, Date Added to IEEE Xplore: 23 January 2020, ISSN: 2150-3699 (electronic). https://doi.org/10.1109/IWSDA46143.2019.8966127 - 18 точки.
    - Borissov, Y. & Markov, M. An Efficient Approach to Point-Counting on Elliptic Curves from a Prominent Family over the Prime Field Fp, Mathematics 2021, 9(12), 1431, ISSN: 2227-7390, https://doi.org/10.3390/math9121431 - 75 точки от IF (Q1).
9. Списък на публикациите по дисертацията:
    1. Borissov, Y. & Markov, M. 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 Proceedings of the 2019 Ninth International Workshop on Signal Design and its Applications in Communications (IWSDA), Dongguan, China, 20–24 October 2019, pp. 1–5, Date Added to IEEE Xplore: 23 January 2020, ISSN: 2150-3680 (print on demand), 2150-3699 (electronic). https://doi.org/10.1109/IWSDA46143.2019.8966127

    2. Markov, M. & Borissov, Y. Point-Counting on Elliptic Curves Belonging to One Prominent Family: Revisited. In Proceedings of the 2020 Algebraic and Combinatorial Coding Theory (ACCT), Bulgaria, 11–17 October 2020, pp. 106–109, Date Added to IEEE Xplore: 25 March 2021, ISBN: 978-1-6654-0288-0 (print on demand), 978-1-6654-0287-3 (electronic). https://doi.org/10.1109/ACCT51235.2020.9383390

3. Borissov, Y. & Markov, M. An Efficient Approach to Point-Counting on Elliptic Curves from a Prominent Family over the Prime Field Fp, Mathematics 2021, 9(12), 1431, ISSN: 2227-7390, IF: 2.3 Q1 (2023), SJR: 0.475 Q2 (2023). https://doi.org/10.3390/math9121431

4. Markov, M. & Borissov, Y. Weight Distribution of the Binary Reed-Muller Code R(4, 9)(4,9). In Proceedings of 2024 The Thirteenth International Workshop on Coding and Cryptography (WCC), Perugia, Italy, 17-21 June 2024, pp. 288–298. https://wcc2024.sites.dmi.unipg.it/WCC_proceedings.pdf

10. Списък на цитиранията на публикациите по дисертацията. Публикация 1 – 1 цитат; публикация 3 – 1 цитат; публикация 4 – 3 цитата.
11. Копия от публикациите по дисертацията – 4 броя по представения списък.
12. Дисертационен труд от 87 страници. Съдържание:
    - Заглавна страница, 2 страници;
    - Декларация за оригиналност, 2 страници;
    - Благодарности, 2 страници;
    - Съдържание, 2 страници;
    - Списък на таблиците, 2 страници;
    - Списък с абревиатури и съкращения, 2 страници;
    - Резюме, 2 страници;
    - Увод, 6 страници;
    - Глава 1 Метод за преброяване на точките върху елиптични криви от вида $y^2 = x^3 + a \pmod p$, $a \neq 0$, 20 страници;
    - Глава 2 Метод за преброяване на точките върху елиптични криви от вида $y^2 = x^3 + ax \pmod p$, $a \neq 0$, 8 страници;
    - Глава 3 Теглово разпределение на двоичния код на Рид-Малер R(4, 9), 24 страници;
    - Библиография, 6 страници, 59 публикации в периода 1896 – 2024;
    - Приложение А: R(4,9) таблици, 4 страници;
    - Приложение Б, 2 страници, терминология;
    - Изнесени доклади по темата на дисертацията, 2 страници, 6 доклада, включително и 4 публикации по дисертацията;

- Публикации по темата на дисертацията, 1 страница, 4 публикации.

13. Справка за приносите в дисертацията и публикациите по дисертацията.
14. Автореферат, 50 страници, на български език.

2. Данни и лични впечатления за кандидата

Образование: Кандидатът завършва средното си образование през 1987 г. в 95 ЕСПУ „Владимир Маяковски“, София. През 1996 г. получава магистърска степен в Техническия университет, инженер по електроника и информатика, специалност Съобщителна и осигурителна техника и системи. През 2006 г. получава бакалавърска степен в СУ „Св. Климент Охридски“, Математика и информатика.

Професионална кариера: От 1992 до 2002 г. работи като командир на екип в Специализирания отряд за борба с тероризма към МВР. От 2002 до 2008 г. е началник на група към Дирекция за защита на средствата за връзка към МВР. От 2008 до 2014 г. е главен експерт към Държавна агенция „Национална сигурност“. От 2022 г. до сега е математик в ИМИ, БАН.

Не познавам лично кандидатът, нито бях запознат с неговата работа преди предзащитата на настоящата дисертация.

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

Дисертацията започва с резюме, в което са представени целта и задачите на изследването. Целта е разработка на ефективни алгоритмични методи за решаването на две специфични задачи: „Преброяване на точките върху елиптични криви“ и „Пресмятане на тегловото разпределение на двоични Рид-Малер кодове“. Задачите са в три групи: за елиптичните криви от семейството $y^2 = x^3 + a \pmod p$, $a \neq 0$, за елиптичните криви от семейството $y^2 = x^3 + ax \pmod p$, $a \neq 0$ и за двоичния код на Рид-Малер $R(4, 9)$. При елиптичните криви се търси извеждане на явна формула за реда на кривата, разработка на ефективен алгоритъм и сравнителен анализ на ефективността с тази на SEA. Задачата за двоичния код на Рид-Малер $R(4, 9)$ е да се намери ефективен алгоритъм за пресмятане на тегловото му разпределение. Резюмето завършва с кратко описание съдържанието на дисертацията.

След резюмето следва Увод, в който са представени основните понятия по тематиката на изследването – за преброяването на точките върху елиптична крива и за теглово разпределение на двоичните кодове на Рид-Малер. Предвид специфичната област на изследване това е добър подход. В отделните глави фокусът е стеснен върху получените резултати. Тук е обоснована стойността на криптирането базирано на елиптични криви. Трябва да се отбележи, че за квантовия компютинг изключително са разчита на този вид криптиране с публичен ключ предвид доказания пробив при традиционния подход.

Глава 1 представя решението на задачите за елиптичните криви от семейството $y^2 = x^3 + a \pmod p$, $a \neq 0$. Изведена е формално явна формула за реда на кривата. Оценена е сложността на пресмятане по получената формула при фиксирано $p \equiv 1 \pmod 6$ и е показано, че тя е с почти два порядъка по-добра от тази на SEA и с един порядък от Munuera, C. & Tena, J. G. An algorithm to compute the number of points on elliptic curves of j-invariant 0 or 1728 over a finite field. Rendiconti del Circolo Matematico di Palermo 42, pp. 106—116 (1993). Експерименталните резултати потвърждават теоретичните изводи за бързодействие. Това със сигурност е потвърдено за SEA, но не и за [Munuera, C. & Tena].

След това в Глава 1 следва изложение на алгоритмите базирани на разработената формула. Кодът на самите алгоритми е публикуван и достъпен в GitHub. Накрая в главата са представени някои конкретни примери с изчисления по представените алгоритми.

Глава 2 е посветена на елиптичните криви от семейството $y^2 = x^3 + ax \pmod p$, $a \neq 0$. Решени са задачите поставени по темата в изследването: изведена е явна формула за реда на елиптичната крива, направена е оценка на сложността на изчисление при $p \equiv 1 \pmod 4$ и е приведен пример за приложението на алгоритъма. Всъщност, сравнението за производителност е със SEA.

Глава 3 е за теглово разпределение на двоичния код на Рид-Малер $R(4, 9)$ с дължина 512 от 4−ти ред. Теоретична обосновка на подхода е направена. Приведени са два алгоритъма за изчисление. Използвани са две мощни изчислителни платформи за изчисление.

Кандидатът разделя получените резултати в две основни категории: научни и научно-приложни приноси.

Научни приноси:

1. Изведена е явна формула за реда на крива от семейството
   $Ep = \{Ea : y^2 = x^3 + a \pmod p, a \neq 0\}$,
   редуциран по модул p.
2. Изведена е явна формула за реда на крива от семейството
   $Dp = \{Da : y^2 = x^3 + ax \pmod p, a \neq 0\}$,
   редуциран по модул p.

Научно-приложни приноси:

1. Разработен е ефективен метод за едновременно пресмятане на шестте възможни реда, свързани със семейството Ep, при фиксирано $p \equiv 1 \pmod 6$. Сложността на този метод е $\tilde{O}(\log_2 p)$, което подобрява най-доброто известно досега алгоритмично решение [3] с почти един порядък.
2. Разработен е ефективен метод за едновременно пресмятане на четирите възможни реда, свързани със семейството Dp, при фиксирано $p \equiv 1 \pmod 4$. Сложността на този метод е $\tilde{O}(\log_2 p)$.
3. Разработен е ефективен алгоритъм за пресмятане на тегловото разпределение на двоичния Рид-Малер код R(4, 9), като е комбиниран подхода, описан в докторската дисертация на D. V. Sarwate [4] от 1973 г., с резултатите за класификацията на Булевите функции според афинната им еквивалентност, публикувани през 2008 г. в [2] и 2023г. в [1].
4. Пресметнато е тегловото разпределение на двоичния Рид-Малер код R(4, 9).

Препратки:

1. Gillot, V. & Langevin, P. Classification of some cosets of the Reed-Muller code. Cryptography and Communications 15, 1129–1137. doi:10 . 1007 / s12095 - 023 - 00652-4 (2023).
2. Langevin, P. & Leander, G. Classification of Boolean Quartic Forms in eight Variables in Boolean Functions in Cryptology and Information Security (eds Preneel, B. & Logachev, O. A.) 18 (IOS Press, 2008), 139–147.
3. Munuera, C. & Tena, J. G. An algorithm to compute the number of points on elliptic curves of j-invariant 0 or 1728 over a finite field. Rendiconti del Circolo Matematico di Palermo 42, 106–116 (1993).
4. Sarwate, D. V. Weight enumeration of Reed-Muller codes and cosets Advisors: E. R. Berlekamp and J. D. Ullman. PhD thesis (Princeton University, Princeton, NJ, Aug. 1973).

Приемам представените научни и научно-приложни приноси, които са подкрепени със съответните препратки.

4. Апробация на резултатите

Дисертацията е оформена на базата на представените четири публикации. Резултатите са публикувани на още два форума освен тези на публикациите по дисертацията.

Публикации [1] и [2] са в IEEE Explore. Публикация [3] е в списание Mathematics с IF и SJR. Публикация [4] е сред приетите резюмета на конференцията, но все още не е публикувана.

Проверих справката за наличните цитати на публикациите по дисертацията. Цитатите по [3] трябва да се отчитат както е посочено в справката по името на идентичната статия в ArXiv макар и с по-различно име: M. Markov, Y. Borissov. Computing the Weight Distribution of the Binary Reed-Muller Code R(4, 9), ArXiv, 2023.

В четирите представени публикации, кандидатът е в съавторство с научния си ръководител, като в две от тях е първи съавтор. Може да се приеме равнопоставеност на приносите.

За покриване на минималните национални изисквания за ОНС „доктор“ се изискат общо 100 точки, като разпределението им по групи показатели е както следва: Група показатели А – 50 точки и група показатели Г – 30 точки. От Група показатели А има 50 точки (представен е дисертационен труд), а от Група показатели Г по показател 7 с публикация [3] има 75 точки (25 х 3 от публикация в издание индексирано в WoS от Q1). Има още точки по представените материали и дори по справката в НАЦИД, но минималните национални изисквания се покриват.

Научните трудове отговарят на минималните национални изисквания (по чл. 2б, ал. 2 и 3 на ЗРАСРБ) и съответно на допълнителните изисквания на БАН и ИМИ, БАН за придобиване на образователна и научна степен „доктор“ в научната област и професионално направление на процедурата.

Представените от кандидата резултати в дисертационния труд и научни трудове към него не повтарят такива от предишни процедури за придобиване на научно звание и академична длъжност.

Няма доказано по законоустановения ред плагиатство в представения дисертационен труд и научни трудове по тази процедура.

5. Качества на автореферата

Представеният автореферат е от 52 страници със съкратено съдържание на дисертацията от 35 страници. В него са представени получените резултати от изследването.

Авторефератът отговаря на изискванията за изготвянето му, както и представя коректно резултатите и съдържанието на дисертационния труд.

6. Критични бележки и препоръки

В Глава 2 са приведени примери за изчисление по получените теоретични резултати, но нищо не е казано за алгоритмизацията и начина на пресмятането им. Липсва публикация на използвания код. Всъщност, алгоритмизацията и кода са почти идентични с този от Глава 1.

В Глава 3 са представени алгоритми за изчисление, но липсва публикация на код. Мотивите за това не са ясни.

Публикуването на кода дава възможност на заинтересованите читатели да проверят получените резултати.

7. 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 научноприложни 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 съответно Правилник за условията и реда за придобиване на научни степени и за заемане на академични длъжности в Българска академия на науките и Правилник за условията и реда за придобиване на научни степени и за заемане на академични длъжности в Института по математика и информатика 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 образователна и научна степен „доктор“ в научна област 4. Природни науки, математика и информатика, професионално направление 4.6. Информатика и компютърни науки.

02 септември 2024 г. Изготвил рецензията:

(проф., д-р Владимир Димитров)