Р Е Ц Е Н З И Я

по дисертационен труд за придобиване на образователна и научна степен "доктор"

по научна специалност „Компютърни системи, комплекси и мрежи"

в професионално направление **5.3 Комуникационна и компютърна техника**

Автор на дисертационния труд: **инж. Димитър Георгиев Тодоров**

Тема на дисертационния труд: „**Изследване на методи за машинно обучение за криптиране на информация**"

Рецензент: **проф. д-р Милена Кирилова Лазарова-Мицева**

катедра „Компютърни системи", Факултет „Компютърни системи и технологии"

Технически университет–София

Настоящата рецензия е изготвена в качеството ми на член на научно жури и рецензент по процедура за защита на дисертационен труд съгласно Заповед №283/10.05.2022 и №326/20.05.2022 на Ректора на Технически университет–Варна и на основание на решение на Катедрения съвет на катедра „Компютърни науки и технологии" (Протокол №21/27.04.2022), решение на Факултетния съвет на Факултета по „Изчислителна техника и автоматизация" (Протокол №24/28.04.2022) и решение от първо заседание на научното жури (Протокол №Д.18.2/13.05.2022).

Рецензията се основава на получени:

- Заповеди №283/10.05.2022 и №326/20.05.2022 на Ректора на Технически университет–Варна;
- Дисертация за придобиване на образователната и научна степен „доктор";
- Декларация за оригиналност на резултатите;
- Автореферат на дисертацията;
- Пълен текст на шест броя научни публикации по темата на дисертацията.

1. Актуалност на разработвания в дисертационния труд проблем в научно и научно-приложно отношение

Дисертационният труд е посветен на безспорно актуална тематика, свързана с прилагането на криптографски методи за сигурен обмен на данни. Широкото приложение на симетрични криптографски алгоритми се дължи основно на тяхното бързодействие и лесното им интегриране в различни системи. С увеличаване на изчислителната мощност на компютърните системи сигурността, която тези алгоритми предоставят, се компрометира при използване на атаки по метода на грубата сила, водещи до проблеми с устойчивостта и дължината на секретния ключ. От друга страна алгоритмите за машинно обучение представляват много актуална област с все по-интензивни научни изследвания в последните години, които водят до успешното им използване за решаване на задачи за класификация и разпознаване в много голям аспект от разнообразни приложни области.

Дисертационният труд успешно комбинира в научно изследване тези две актуални области като предлага използването на методи за машинно обучение за създаване и обучение на модели за класификация и разпознаване на секретни ключове от симетрични криптографски алгоритми с цел повишаване на устойчивостта им.

Целта на представения за рецензиране дисертационен труд е насочена към постигане на по-висока устойчивост на симетричните криптографски алгоритми чрез проучване, анализ и изследване на методи и алгоритми за машинно обучение за анализ и предсказване на вида на алгоритъма, към който принадлежи даден секретен ключ, посредством обучаващи данни подходящи по тип, вид и обща големина. Във връзка с поставената цел и на базата на анализ на текущото състояние на проблемната област са формулирани конкретни задачи, свързани с целта на дисертационния труд: „(1) Да се проучат съществуващите методи и алгоритми за машинно обучение за извличане на знания и анализ на масиви от данни; (2) Да се анализират и подберат подходящ по тип, вид и обща големина обучаващи данни за алгоритмите на машинно обучение. Да се предложи алгоритъм, осигуряващ подходящ вид на входните данни за алгоритмите за машинно обучение; (3) Да се проектира и разработи софтуерен модел (приложение) за разпознаване на симетрични криптографски алгоритми чрез машинно обучение, което да се използва за провеждане на експериментални проучвания, както за целите на дисертацията, така и за бъдещи потребности в учебни и приложни процеси; (4) Да се оцени експериментално възможността за използване на методи и алгоритми за машинно обучение за обработване, анализ и класификация на криптографския ключ и увеличаване на устойчивостта на симетричните криптографски алгоритми“. Определянето на целта и конкретните задачи, свързани с постигането ѝ, са обосновани от автора коректно и изчерпателно.

2. Степен на познаване състоянието на проблема и творческа интерпретация на литературния материал

Дисертационният труд обхваща тематика, която включва необходимост от познаване на методи и алгоритми за машинно обучение и използването на машинно обучение за създаване и обучение на модели за класификация и разпознаване на секретни ключове от симетрични криптографски алгоритми с цел повишаване на устойчивостта им. Авторът на дисертационния труд показва висока степен на познаване на актуалното състояние на поставения за решаване проблем, за което свидетелства обстойна литературна справка и творческа интерпретация на съвременното състояние на проблемната област. Направеният литературен обзор е базиран на голям брой използвани литературни източници. Литературното проучване е в основата на формулираната цел и свързаните с нея задачи за постигането ѝ. Библиографската справка и цитираните литературни източници, на които е базиран сравнителния литературен анализ, обхващат научни изследвания и статии в научни издания и международни конференции, като над 80% от тях са публикувани в последните 10 години, а около 46% от цитираните от автора научни публикации са от последните 5 години.

3. Съответствие на избраната методика на изследване с поставената цел и задачи на дисертационния труд

Избраната методика за изследване, поставената цел, както и формулираните задачи за постигането на целта, съответстват на темата на дисертационния труд и на постигнатите резултати и приноси. Избраната методика за провеждане на научните изследвания се базира на системен сравнителен анализ на особеностите и различните аспекти на разглежданата тематична област. Предложените, разработени и изследвани модели се основават на аргументиран избор, теоретична обосновка, експериментална оценка и верификация на възможностите за използването им. За апробиране на резултатите от научното изследване са използвани техники за моделиране и прилагане на статистически и аналитични методи за обработване на данни.

Методически дисертационният труд е логически последователен и адекватен по отношение на избраната и приложена методика на провеждане на научните изследвания, което обуславя успешно изпълнение на поставените цел и задачи на дисертационния труд.

4. Кратка аналитична характеристика и оценка на достоверността на материала, върху който се градят приносите на дисертационния труд

Представеният за рецензия дисертационен труд е с общ обем 137 страници, структуриран в увод, четири глави, заключение, списък с приноси по дисертационния труд, списък с публикации на докторанта по дисертационния труд, списък с участия в научно-изследователски проекти, списък с фигури и графики, списък с таблици и библиографска справка на цитираните литературни източници. В текста са използвани 64 фигури, 10 графики и 16 таблици. Посочени са общо 121 литературни източници, от които 11 на кирилица и 110 на латиница.

В първа глава на дисертационния труд е представен обзорен преглед на съществуващите и използвани криптографски алгоритми с акцент върху алгортими за симетрична криптография, както и на някои от най-известните и популярни алгоритми за машинно обучение, приложими за решаване на различни криптографски задачи. Втора глава съдържа описание на предложения в дисертационния труд подход за повишаване на устойчивостта на симетрични криптографски алгоритми чрез машинно обучение. Трета глава описва предложеното решение на проблема с устойчивостта на симетрични криптографски алгоритми чрез машинно обучение, както и предложения от автора алгоритъм за поставяне на данни в еднородна среда. Представени са разработените програмни среди за тестване на предложените алгоритмични решения. В четвърта глава са анализирани резултати от експериментални изследвания за оценка на ефективността на предложения в дисертационния труд подход за повишаване на устойчивостта на симетрични криптографски алгоритми чрез машинно обучение.

От представеното изложение, формулираната цел на дисертационните изследвания и поставените във връзка с нея задачи, както и използваните средства за постигане на целта, може да се направи заключение, че докторанта добре познава състоянието на разглежданите проблеми. Представените подходи са верифицирани чрез експериментални изследвания и е анализирана приложимостта им. Това ми дава основание да определя получените резултати и свързаните с тях приноси като достоверни и практически полезни.

5. Научни и научноприложни приноси на дисертационния труд

Приемам формулираните от автора приноси, които са обобщени в дисертационния труд и могат да бъдат систематизирани като научни, научно-приложни и приложни приноси както следва:

- ***научни приноси:***

• Предложен е алгоритъм за поставяне на данни в еднородна среда, осигуряващ подходящ вид на входните данни за обучение на алгоритми за машинно обучение;

• Предложен е подход за формиране на обучаващо множество за класифициране на криптографски данни с помощта на предложения алгоритъм за поставяне на данни в еднородна среда;

- ***научно-приложни приноси:***

• Предложен е подход за проектиране, конфигуриране и имплементиране на предложения алгоритъм за поставяне на данни в еднородна среда и алгоритми за машинно обучение за разпознаване на криптографски данни;

- ***приложни приноси:***

• Предложеният алгоритъм за поставяне на данни в еднородна среда е реализиран заедно с алгоритми за машинно обучение kNN и SVM в система за разпознаване на криптографски данни;

• На базата на експериментални изследвания са определени подходяща конфигурация и параметри на модел за класификация на криптографски данни с цел увеличаване на устойчивостта на симетричните криптографски алгоритми. Определен е размера на еднородната среда в зависимост от дължината на симетричния ключ;

• С използване на разработената система за разпознаване на криптографски данни е предоставена възможност за реализиране на модел на многопрофилно криптиране или криптиране с различни алгоритми в единна среда.

Приносите могат да се отнесат към категориите обогатяване на съществуващо научно знание и научни постижения в практиката, както и създаване на нови и модифициране на съществуващи методи, подходи, модели и алгоритми за решаване на поставените в дисертационния труд задачи.

6. Оценка за степента на личното участие на дисертанта в приносите

Представеното съдържание и структура на дисертационния труд показват отличното познаване на третираната проблематика от страна на докторанта. В пет от публикуваните шест научни статии във връзка с дисертацията докторанта е водещ автор. Представените материали по дисертационния труд и публикациите към него правят добро впечатление за научната работа на докторанта, която се характеризира със задълбоченост и прецизност. Считам, че личния му принос при постигане на резултатите по дисертационния труд е безспорен.

7. Преценка на публикациите по дисертационния труд

Получените от автора резултати от дисертационното изследване са публикувани в шест научни статии. Една от публикациите е представена на международна научна конференция я чужбина, 2 от статиите са докладвани на международни научни конференции, проведени в България, които са индексирани в Scopus, 3 статии са публикувани в научни списания в България. Публикациите са направени в периода 2017–2022 година и покриват тематиката на представената дисертационна работа като отразяват основните постигнати резултати и приноси. Не са представени данни за забелязани цитирания на публикациите по дисертационния труд.

8. Използване на резултатите от дисертационния труд

Не са представени данни за практическо използване на получените резултати от научните изследвания в дисертационния труд, но във връзка с научните изследвания по дисертационния труд докторантът е участвал в три научно-изследователски проекта, финансирани от НИС при ТУ–Варна. Постигнатите резултати имат значение освен от гледна точка на получените научни, научно-приложни и приложни приноси, но и поради възможността за използването им за бъдещи научни изследвания. Практическата ценност на изследването се основава на възможността за приложно практическо използване на предложените подходи и алгоритми за анализ и класификация на шифротекстове с цел разпознаване на криптиращия алгоритъм за постигане на криптографска комуникация без „уговорка“ между подател и получател за вида на ключа и без необходимост от съхранение на секретен ключ.

На базата на получените в дисертационния труд резултати може да бъде разработен реален приложен продукт, достъпен за масово потребителско използване, позволяващ прилагането на класификационен модел при многопрофилно криптиране или криптиране с различни алгоритми.

9. Препоръки за бъдещо използване на научните и научно-приложните приноси на дисертационния труд

Препоръчвам на докторанта да продължи научните си изследвания по темата на дисертационния труд, като ориентира научната си и публикационна дейност към международни издания и участия в международни научни проекти, както и към практическа реализация с възможности за внедряване на получените резултати в реални проекти и постигане на преки приложни резултати.

10. Оценка на съответствието на автореферата с дисертационния труд

Авторефератът към дисертацията съответства на дисертационния труд – вярно и точно отразява целите, задачите, съдържанието по глави, постигнатите приноси. Авторефератът е подготвен и оформен съгласно изискванията за изготвянето му и считам, че безспорно носи същностните черти на дисертационния труд, като отразява в адекватен обем и по коректен начин неговото съдържание.

11. Критични бележки

Нямам забележки към дисертационния труд. Той е оформен внимателно и старателно с високо ниво на представяне на научните изследвания, свидетелства за добро запознаване на автора с предметната област. Разглежданата тематика касае много актуална област, към която са насочени значителни усилия на редица изследователи. Авторът е изпълнил поставените цел и задачи в дисертационния труд, на базата на което са постигнати научни, научно-приложни и приложни приноси. Считам, че приносите, за които автора претендира, са значими и биха могли да имат бъдещо практическо приложение. Съществените приноси на дисертационния труд са отразени в научни публикации, които са направени достояние на заинтересованата научна общност.

12. Заключение

На основание на изложеното считам, че дисертационния труд напълно отговаря на изискванията на Закона за развитие на академичния състав в Република България, на Правилника за прилагане на закона и съответния правилник на Технически университет–Варна, както и на изискванията за придобиване на образователната и научна степен „доктор”.

Ето защо убедено давам своята положителна оценка на представения дисертационен труд и предлагам на уважаемите членове на Научното жури да бъде присъдена образователната и научна степен „доктор” на **инж. Димитър Георгиев Тодоров** по научна специалност „Компютърни системи, комплекси и мрежи“ в професионално направление 5.3 Комуникационна и компютърна техника.

17.06.2022 г. **Рецензент:**

/ проф. д-р Милена Лазарова–Мицева /