РЕЦЕНЗИЯ

от д.н. Борислав Панайотов Стоянов, професор в Шуменския университет, ФМИ

на дисертационен труд за присъждане на образователната и научна степен **„доктор“**

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

професионално направление 4.6 Информатика и компютърни науки,

докторска програма Информатика

Автор: Тони Пламенов Каравасилев

Тема: „Софтуерна рамка за криптографски услуги“

Научни ръководители: проф. д-р Елена Петрова Сомова и доц. д-р Светослав Христосов Енков, ПУ „Паисий Хилендарски“- ФМИ

1. Общо описание на представените материали

Със заповед № Р33-5350 от 22.10.2021 г. на Ректора на Пловдивския университет „Паисий Хилендарски" (ПУ) съм определен за член на научното жури за осигуряване на процедура за защита на дисертационен труд на тема „Софтуерна рамка за криптографски услуги“ 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, докторска програма Информатика. Автор на дисертационния труд е Тони Пламенов Каравасилев – докторант в редовна форма на обучение към катедра Компютърна Информатика с научни ръководители проф. д-р Елена Петрова Сомова и доц. д-р Светослав Христосов Енков от ПУ „Паисий Хилендарски“- ФМИ.

Представеният от Тони Пламенов Каравасилев комплект материали на хартиен носител е в съответствие с Чл.36 (1) от Правилника за развитие на академичния състав на ПУ, включва следните документи:

- молба до Ректора на ПУ за разкриване на процедурата за защита на дисертационен труд;
- автобиография в европейски формат;
- протокол от катедрения съвет, свързан с докладване на готовността за откриване на процедурата и с предварително обсъждане на дисертационния труд;
- дисертационен труд;
- автореферат;

- списък на научните публикации по темата на дисертацията;
- копия на научните публикации;
- списък на забелязани цитирания;
- декларация за оригиналност и достоверност на приложените документи;
- справка за спазване на специфичните изисквания на съответния факултет (само за докторантите зачислени до 04.05.2018 г.);
- справка за спазване на минималните националните изисквания за придобиване на ОНС "доктор" по ПН 4.6. Информатика и компютърни науки.

Докторантът е приложил 4 публикации и списък с 4 забелязани.

2. Кратки биографични данни

Тони Каравасилев е роден на 1 април 1992 г. През 2016 г. Завършва магистратура по специалност "Софтуерни технологии" в ПУ. Понастоящем работи в софтуерна фирма като старши програмист, уеб приложения. Владее немски и английски език.

3. Актуалност на тематиката и целесъобразност на поставените цели и задачи

В следствие на изискването от различни криптографски услуги и примитиви за автентикация, генериране на идентификатори, криптиран трафик, механизми за размяна на сигурни съобщения, проверки за целостта на информацията или методи за безопасно складиране на данни от тип парола, кредитна карта или дори файлове, като изображения или документи, за осъществяване на сложни взаимодействия или комбинации от различните типове алгоритми за информационна сигурност изниква необходимостта от осъществяване на сложни взаимодействия или комбинации от различни типове алгоритми за информационна сигурност.

4. Познаване на проблема

В първа глава на дисертационния труд е направен подробен анализ на криптографската област. Изяснени са основните понятия и изисквания в криптографския модел. Изведена е йерархия от абстракции за криптографските грешки, грешки за алгоритми, грешки при идентификация, грешки при автентикация и грешки при авторизация. Всичко това налага проектиране на софтуерна рамка, чрез предварителен анализ и подбор на функционалните изисквания за съответната архитектура.

5. Методика на изследването

За реализиране на изследването е извършено проектиране, реализация, тестване и техническо документиране на софтуерна рамка. Извършен е анализ на приложимостта на изградения модел.

6. Характеристика и оценка на дисертационния труд

Представеният дисертационен труд се състои от увод, четири глави и заключение, списък на използваната литература, списък на авторските публикации по темата, приложения и декларация за оригиналност. Съдържа разработена методика за реализация и интеграция на криптографски услуги чрез цялостна софтуерна рамка за осигуряване на сигурността на съвременните информационни системи, както и анализ на качеството на използвания криптографски модел на базата на съществуващи разработки реализирани на различни езици за програмиране и видове платформи.

В Първа глава се разглеждат теоретичните основи на криптографията и различните видове криптографски системи, както и използваните в съвременната практика стандарти. Направен е обзор на най-ефективните подходи за проектиране, реализиране и документиране за софтуерни рамки.

Във Втора глава се разглеждат в детайли процесите по проектиране на абстрактния криптографски модел и специализираната софтуерна рамка за криптографски услуги. Тази глава включва функционален анализ и сравнение на приложимостта на проектираната софтуерната рамка спрямо група от конкурентни софтуерни разработки за различни платформи.

В Трета глава се разглеждат в детайли реализацията, тестването, документирането и публикуването на софтуерната рамка за криптографски услуги. Тя включва всички технически детайли по изграждането на нейния цялостен криптографски модел чрез PHP.

В Четвърта глава се дефинират абстрактни методологии за подсигуряване на информационни системи, изцяло реализуеми чрез интеграцията на изградената софтуерна рамка за криптографски услуги. Тази глава включва обзор на най-ефективните практики и съвети за постигане на цялостна защита на данните по време на техния пренос и съхранение, както и разглежда редица алтернативни методи за постигане на сигурна комуникация между множество страни.

В Заключението са систематизирани получените резултати и са изброени научно-приложните и приложните приноси на дисертационния труд. Очертани са бъдещите насоки за развитието на софтуерната рамка и нейния абстрактен криптографски модел.

Основният текст на дисертацията от 165 страници и съдържа 9 приложения. Списъкът на използваната литература е от 117 заглавия и 29 уеб базирани източници.

7. Приноси и значимост на разработката за науката и практиката

Основните приноси на дисертацията могат да се характеризират като научно-приложни и приложни. С нейна помощ всеки един ново-разработван или вече съществуващ софтуерен продукт може да интегрира криптографски услуги и изгради адекватна цялостна защита на базата на най-ефективните практики в сферата на сигурността.

Проектантите и програмистите на софтуерни системи могат да използват създадените методики по време на разработването или поддръжката на своите продукти, за да покрият всички изисквания за нивото на сигурност, поставени от регулаторите или нуждите, дефинирани от потребители им.

Научно-приложните приноси са:

- Създаден е общ, платформено независим криптографски модел за представяне на криптографски примитиви и услуги;
- Създадени са методики (набор от препоръки, правила, инструменти и съвети) за осигуряване на защита на информационни системи в различен приложен контекст;
- Проектирана е софтуерна рамка за криптографски услуги на базата на анализ на съществуващи решения от различни технологични среди;
- Предложена е унифицирана архитектура за управление на криптографски услуги и примитиви чрез платформено независим подход за реализация.

Приложните приноси са:

- Реализирана е софтуерна рамка за криптографски услуги като приложен инструмент за създаване, управление и конфигуриране на сигурни софтуерни услуги и среди;
- Интегриран е криптографски модел в език за програмиране без наличието на вградена поддръжка на криптографски услуги и примитиви;
- Извършено е тестване на създадената софтуерна рамка, автоматизирано и с реални потребители, и е направен анализ на получените резултати.

Моделите на методики и софтуерните средства, създадени в рамките на дисертацията, са използвани за създаване на учебния курс ИД Приложна криптография в Интернет с PHP.

8. Преценка на публикациите по дисертационния труд

По дисертационния труд са направени 5 (пет) публикации в реферирани и индексирани издания. Една от тях е в сборника IOP Conference Series: Materials Science and Engineering, който е индексиран в Scopus с SJR за съответната 2019 година от 0.198. С това се покриват Минималните национални изисквания, а също така и специфичните такива на ФМИ при ПУ.

Три от публикациите са с научния ръководител доц. д-р С. Енков, една с втория научен ръководител доц. д-р Е. Сомова и една е самостоятелна.

Представена е информация за известни общо 4 (четири) цитирания на две от публикациите по дисертационния труд. Отличавам цитата от списание Journal of Software: Evolution and Process, което е с IF 1.972.

9. Лично участие на докторанта

Смятам, че личното участие на докторанта във всички етапи от представеното дисертационно изследване е безспорно, разбира се под ръководството на научните ръководители. Постигнатите научно-приложни и приложни резултати са получени в изпълнение на поставените задачи вследствие на научното ръководство и са лично дело на докторанта.

10. Автореферат

Внимателно се запознах с автореферата и смятам, че той вярно и точно отразява основните моменти от дисертационния труд, в разумен и подходящ обем и съдържание, като в същото време представлява самостоятелна публикационна единица.

11. Критични забележки и препоръки

Имам следната препоръка относно бъдещите изследвания на докторант Тони Каравасилев: в продължение на обектноориентираното моделиране за постигане на пълнота при изследването на псевдослучайни редици е необходимо да се изчисли големината на ключовото пространство, да се анализират хистограмите, да се изследва уязвимостта на криптоанализ и да се направят статистически тестове с пакети ENT, DieHarder, NIST test suite и др.

12. Лични впечатления

Не познавам лично докторант Тони Каравасилев и нямам преки впечатления от неговата работа. Изводите ми, относно дисертационно изследване, са направени изключително само от предоставените материали по процедурата.

13. Препоръки за бъдещо използване на дисертационните приноси и резултати

Препоръчвам публикуване на резултатите от дисертационното изследване в издания с импакт фактор, тъй като естеството на изследванията позволява достигането на това ниво.

ЗАКЛЮЧЕНИЕ

Дисертационният труд ***съдържа научно-приложни и приложни резултати, които представляват оригинален принос в науката*** и **отговарят на всички** изисквания на Закона за развитие на академичния състав в Република България (ЗРАСРБ), Правилника за прилагане на ЗРАСРБ и съответния Правилник на ПУ „Паисий Хилендарски“. Представените материали и дисертационни резултати напълно съответстват на специфичните изисквания на Факултета по математика и Информатика, приети във връзка с Правилника на ПУ за приложение на ЗРАСРБ.

Дисертационният труд показва, че докторантът Тони Пламенов Каравасилев притежава задълбочени теоретични знания и професионални умения по докторската програма Информатика в професионалното направление 4.6.Информатика и компютърни науки, като демонстрира качества и умения за самостоятелно провеждане на научно изследване.

Поради гореизложеното, убедено давам своята ***положителна оценка*** за проведеното изследване, представено от рецензираните по-горе дисертационен труд, автореферат, постигнати резултати и приноси, и ***предлагам на почитаемото научно жури да присъди образователната и научна степен „доктор“*** на Тони Пламенов Каравасилев в област на висше образование 4. Природни науки, математика и информатика, професионално направление 4.6 Информатика и компютърни науки, докторска програма Информатика.

21.11.2021 г. Рецензент:

(проф. д.н. Борислав Стоянов)