С Т А Н О В И Щ Е

от проф. д-р Маргарита Теодосиева,
Русенски университет „А. Кънчев“

на дисертационен труд за присъждане 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*

Автор: **Михаела Димитрова Тодорова**
Докторант към катедра *Компютърна информатика* при факултет *Математика и информатика* на Шуменския университет „Епископ Константин Преславски“, отчислена с право на защита със заповед No РД-10-335/22.02.2019 г. (считано от 1.02.2019 г.)

Тема: **Изследване на хешираща функция за информационна защита**

Със заповед на Ректора на Шуменския университет съм определена за член на научното жури за защита на дисертационен труд на тема *Изследване на хешираща функция за информационна защита* 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* на докторанта ***Михаела Димитрова Тодорова.*** Настоящето становище е изготвено на основание на ЗРАСРБ, Правилника за неговото приложение, както и Правилника на Шуменския университет.

Дисертацията е разработена под научното ръководството на проф. д.н. Борислав Панайотов Стоянов и проф. д.н. Кшищов Станислав

Шчипьорски.

При реализирането на процедурата за публична защита на дисертационния труд няма допуснати нарушения, за което съдя от предоставената ми документация.

1. Кратки биографични данни

След прилючване на средното си образование в Природоматематическата гимназия „Акад. Никола Обрешков“, гр. Бургас за една година ***Михаела Тодорова*** е изучавала специалност *Компютърни науки* в Софийския университет. Веднага след завършване на бакалавърската специалност *Компютърна информатика* през 2014 г. в Шуменския университет тя продължава обучението си в магистърската програма *Софтуерно инженерство*, която завършва през 2015 г.

В периода 02.2016 – 02.2019 ***Михаела Тодорова*** е редовен докторант в катедра *Компютърна информатика* при Шуменския университет.

Трудовата си дейност започва през октомври 2015 г. като асистент по информатика в Шуменския университет, владее програмните езици C++ и Java, и е участвала в 4 научно-изследователски проекти. Има общо четири публикации, три доклади и една цитирана публикация. Владее немски, английски и руски езици, които използва в своята научна дейност.

2. Общо описание на дисертационния труд и на приложените към него материали

Представеният за рецензиране дисертационен труд от 108 страници се състои от увод, три глави, всяка от които завършва с изводи, заключение и библиография. Литературните източници са 136, от които 96 на латиница и 12 на кирилица. За онагледяване в изложението са представени 22 фигури и 45 таблици.

Дисертационният труд е балансиран, с последователна научно-

изследователска логика, подчинена на ясно формулирани цел и задачи, като структурата и съдържанието му отговарят на изискванията на ЗРАСРБ и Правилника за неговото приложение.

Авторефератът е в обем от 38 страници, в които са включени вижданията и насоките за по-нататъшна работа, списъкът на използваните съкращения, както и списъкът с публикациите. В автореферата не е посочена цитираната литература, но номерацията на библиографията съвпада с тази от дисертационния труд, което е индикация за добра систематичност и научна прецизност.

Въпреки малкия обем авторефератът е написан съгласно изискванията, издържан е в структурно отношение, дава достатъчно добра и ясна представа за разглежданата от докторанта проблематика и отразява логиката и последователността на дисертационния труд,

3. Актуалност на проблема

Актуалността на разработваната дисертация е очевидна - конструирането на нови криптографски хеш-функции за осигуряване безопасността на предаваните сигнали е актуален научен проблем.

4. Познаване състоянието на проблема

Докторантката е навлязла професионално в проблематиката и показва познаване състоянието на научните проблеми и специфичните особености на предметната област като едновременно е обогатила знанията си по темата и е създала добре подплатени с аргументи изводи, както и научни и научно-приложни приноси. Списъкът с научни източници несъмнено сочи сериозна подготовка - цитираните в дисертацията библиографски източници са показател за равнището на труда, съответстващо на научната степен „доктор“.

5. Подход и решение на проблема

Главната цел на научното изследване е разработването и изследването на хешираща функция за информационна защита, чрез използване на математически функции от теорията на хаоса и Бент булеви функции, които се подлагат на различни филтри. За постигане на така поставената цел е предвидено решаването на няколко **задачи,** по които последователно и методично е работено: да се анализира текущото състояние на развитие на хеширащите функции за информационна сигурност; да се моделират и изследват алгоритми за получаване на псевдослучайни двоични редици с използване на математически функции от теорията на хаоса; да се моделират и изследват криптографски хеширащи алгоритми за информационна защита. **Обект** на изследването е подходящата за включване в системата за информационна защита хешираща криптографска функция. **Предмет** на дисертационното изследване са аналитичните и статистическите свойства на хеширащите функции.

Съдържанието на **Първа** глава *Съвременно състояните на проблема свързан с криптографските хеш алгоритми*, показва, че изборът на темата на дисертацията е сполучлив. Прави впечатление задълбоченият и пълен анализ на състоянието на изследванията в областта на представената тематика. Тук са представени основните понятия в криптографията, криптографската система, както и криптографските примитиви и механизми. Разгледани са симетричните и асиметричните криптографски алгоритми. Описани са криптографските хеш алгоритми: същността, видовете и основните характеристики на хеш-функциите.

Във **Втора** глава *Псевдослучайни генератори, базирани на хаотични системи* са разгледани същността и видовете псевдослучайни генератори - сумиращи и свиващи псевдослучайни генератори чрез преместващи регистри, самосвиващи псевдослучайни генератори, псевдослучайни

генератори, базирани на хаотични системи, както и Бент булевите функции;т емата за псевдослучаен битов генератор, базиран на неравномерно филтриране на хаотично изображение, описва Tinkerbell map и модела на псевдослучайния генератор. Тестовете на псевдослучайния генератор включват колизия на пространство от ключове и статистически тест. Отделено е място и на псевдослучайна конструкция на битовете, базирана на хаотичен атрактор – дадени са описанието на Signature атрактор, моделът и тестовете на генератора, анализът на пространството от ключове и статистическите тестове.

Трета глава *Разработване и изследване на хешираща функция за информационна защита* е най-съществената част от дисертацията. За изясняване на базираната на неравномерно филтриране на хаотично изображение Хеш-функция е разгледан моделът на хеш-функцията и е проведено изследване на предложения модел, включващ дистрибутивен анализ, анализ на чувствителността, статистически анализ на конфузия и дифузия и анализ на колизиите. Хеш алгоритъмът, базиран на Бент булева функция и хаотичен атрактор, е представен с описание и изследване на модела на хеш-функцията. Приложени са: дистрибутивен анализ, анализ на чувствителността, статистически анализ на конфузия и дифузия, анализ на колизиите, анализ на Birthday атака, анализ на Meet-in-the-Middle атака (човек в средата) и анализ на Second Pre-Image атака.

Теоретичните и експерименталните резултати за двата хеширащи алгоритъма потвърждават високото ниво на сигурност, с възможност за практическо реализиране в софтуерни приложения.

В **Заключението** се подчертава, че в рамките на дисертационно изследване са решени поставените задачи и са формулирани основните научни и научно-приложни приноси. Дадени са виждания и насоки за по-нататъшна работа.

6. Достоверност на получените резултати и публикации по темата

В трите публикациите на докторантката са отразени някои от основните резултати, получени в дисертационния труд, които не подлежат на съмнение и може да се счита, че резултатите са апробирани пред специализирана научна адитория. Всички публикации вече са излезли от печат. Две от публикациите са на английски език (първата е в списание индексирано от Scopus, втората е в списание с Impact Factor), а третата е на български и докторантката е единствен автор в нея. Публикациите са напълно достатъчни за получаване на ОНС „доктор".

7. Основни приноси на дисертационния труд

Проведените експерименти и получените резултати показват ползите от проведеното дисертационо изследване и довеждат до 2 научни и 4 научно-приложни приноси, които одобрявам и приемам без промяна.

8. Заключение

Предвид всичко гореизложено съм убедена, че представеният дисертационен труд отговаря на изискванията на ЗРАСРБ, Правилника за неговото приложение и Правилника на Шуменския университет, и му давам положителна оценка.

Предлагам на уважаемото научно жури да присъди на **Михаела Димитрова Тодорова** образователната и научна степен „доктор" в област на висше образование 4. Природни науки, професионално направление: 4.6. Информатика и компютърни науки, докторска програма *Информатика*.

24 юли, 2019 г. Изготвил становището:

/проф. д-р М. Теодосиева/