ШУМЕНСКИ УНИВЕРСИТЕТ
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

Р Е Ц Е Н З И Я

от професор д.т.н. Веселин Целков

КОМИСИЯ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

на дисертационен труд на доц. д-р Борислав Панайотов Стоянов на тема „Криптографски алгоритми за защита на информацията”, за придобиване на научната степен „доктор на науките”

Шумен
2015 г.

1. ОБЩО ПРЕДСТАВЯНЕ НА ПОЛУЧЕНИТЕ МАТЕРИАЛИ

За рецензия са ми представени следните материали:

- Дисертационен труд за придобиване на научна степен „доктор на науките" на тема: „Криптографски алгоритми за защита на информацията", с автор доц. д-р Борислав Панайотов Стоянов – 187 стр.;
- Автореферат на дисертационния труд – 56 стр.;
- Списък и копия от публикациите по темата на дисертацията – 27 бр., от които:
  - Осем (8) на български;
  - Деветнадесет (19) на английски;
- Справка с приносите;
- Справка за известните цитирания на публикациите по темата на дисертацията – 37 бр.

Приемам за рецензия всички предложени доклади, публикации, разработки и учебни пособия като съответстващи към темата на дисертационния труд. Анализирайки представените ми документи по обем и съдържание, може да се направи изводът, че те са достатъчни за представяне и изясняване на получените научни, научно-приложни и приложни резултати.

Авторефератът на дисертационния труд удовлетворява изискванията на закона за съдържание и оформяне.

2. АКТУАЛНОСТ И ЗНАЧИМОСТ НА РАЗРАБОТВАНИЯ В ДИСЕРТАЦИОННИЯ ТРУД ПРОБЛЕМ

Развитието на информационните технологии и навлизането им във всички области на обществения и личен живот поставят нови предизвикателства за защита на информацията, обработвана в компютърните системи и мрежи. Съществуват различни технологични решения за защита на информацията, но безспорно най-ефективното и сигурно решение е използването на

криптографски алгоритми и механизми в системата за защита на информацията. Ето защо формулираната от кандидата цел: „Разработване и изследване на нови криптографски алгоритми за защита на информацията чрез използване на следните градивни елементи:

- Линейни преместващи регистри с обратна връзка;
- Преместващи регистри с обратна връзка и пренос;
- Бент функции и хаотични функции"

е актуална и съвременна. Това се доказва и прецизира и от задачите, които са решени:

- Изследване и разработване на криптографски алгоритми за генериране на псевдослучайни числа на основата на преместващи регистри с обратна връзка;
- Изследване и разработване на криптографски алгоритми за генериране на псевдослучайни числа чрез нелинейни динамични системи;
- Изследване и разработване на криптографски алгоритми за защита на изображения.

Тези изследвания биха могли да имат непосредствено приложение в конкретни технологични решения за защита, а така също могат да бъдат в основата на различни университетски образователни курсове – като съдържание и методика на изследването.

3. АНАЛИТИЧНА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Описание на дисертационния труд

Представеният ми за рецензиране труд е структуриран в увод, четири глави, заключение и списъци с фигури, таблици, алгоритми, и използваната литература.

В увода е обоснована актуалността на изследването, специфицирани са предметът и обектът на изследването, дефинирани за целта и задачите му.

Всичко това дава възможност да се получи ясна представа за характера и съдържанието на дисертационното изследване.

Глава първа е посветена на „Генериране на псевдослучайни двоични последователности чрез регистри с обратна връзка". Направен е увод в криптографията и криптографските системи, направен е аналитичен анализ на използването за целта на преместващи регистри с обратна връзка, представено е моделиране на сумиращи псевдослучайни генератори чрез преместващи регистри и моделиране на свиващи псевдослучайни генератори чрез преместващи регистри. На базата на това са изведени и дефинирани основни свойства, които следва да притежават псевдослучайни двоични редици, за да удовлетворят изискванията за устойчивост на криптоатака.

Глава втора е посветена на генериране на самосвиващи псевдослучайни битови последователности чрез преместващи регистри с обратна връзка. Синтезиран е самосвиващ се генератор, изпълнен с преместващ регистър с обратна връзка и пренос. Предложени са:

- Самосвиващ генератор на основата на 2-адичен преместващ регистър с обратна връзка и пренос и свиващата функция на Jabri;
- Редактиращ битове-търсещ генератор на базата на преместващ регистър с обратна връзка и пренос.

Разработени са математически модели за доказателство на ефективността на предложените решения.

В глава трета са разгледани въпросите свързани с генериране на псевдослучайни последователности с използване на нелинейни динамични системи, като са разработени множество от псевдослучайни генератори, както следва:

- Псевдослучаен генератор на битове, базиран на стандартно кръгово изображение;
- Псевдослучаен генератор на битове, базиран на стандартно изображение на Chirikov, филтрирано чрез свиващо правило на Jabri;
- Генератор, базиран на изображението на Zaslavsky;

4. ПРИНОСИ В ДИСЕРТАЦИОННИЯ ТРУД И НА ПУБЛИКАЦИИТЕ ПО НЕГО

Приносите на кандидата могат да бъдат отнесени в област на висшето образование 4. Природни науки, математика и информатика, към професионално направление 4.6. Информатика и компютърни науки, научна специалност Информатика. Публикуваните резултати най-общо могат да бъдат разделени на научни и научно-приложни.

Научни приноси

Научните приноси са свързани с изследване и разработване на нови криптографски алгоритми и методи. Научните приноси на кандидата могат да бъдат рецензирани и оценени в следните направления:

- Обогатяване на съществуващите знания;
- Приложение на научни постижения в практиката и реализиран икономически ефект.

Научно-приложни приноси

Научно-приложните приноси са в областта на синтезирането на нови криптографски алгоритми, нови методи и приложението им за защита на изображения. Доказателство за това са разработените и реализирани проекти, финансирани от Фонд Научни изследвания и Оперативна програма Развитие на човешките ресурси.

Приемам приносите така, както са предложени от кандидата. Считам, че представените публикации пълно и точно отразяват количеството и качеството на изследванията представени за рецензиране.

5. АВТОРСКО УЧАСТИЕ

Научната и преподавателската дейност на доц. д-р Борислав Панайотов Стоянов го характеризират като добър преподавател, последователен учен, с трайни интереси в криптографията и нейното приложение.

- Псевдослучаен генератор, базиран на изображението на Chebyshev;
- Псевдослучаен генератор, базиран на изображението на Duffing.

Всички синтезирани генератори са изследвани и е доказана тяхната ефективност чрез разработени за целта математически модели.

Глава четвърта е посветена на защитата на изображения посредством криптографски алгоритми. За целта са разработени, апробирани и с доказана ефективност следните методи:

- Метод за защита на изображения чрез преместващ регистър с обратна връзка и пренос, филтриран чрез функцията на Jabri;
- Метод за защита на изображения посредством изображенията на Duffing и Chebyshev.

Аналитична характеристика на дисертационния труд

Аналитичния анализ на предложения дисертационен труд води до извода за неговата завършеност и възможност за практическата приложимост на представените резултати. Това се определя и от постановката на задачата и от начините на формализиране и търсене на решения. Предметната област, свързана с разработването и прилагането на криптографски алгоритми, е строго специфична и изисква задълбочена теоретична подготовка и богат практически опит в защитата на информацията. Предлагането на нови решения за постигане на целта на дисертационното изследване затвърдява представата за значимост на получените резултати за нуждите на теорията и на практиката.

Считам, че обемът и съдържанието на дисертационния труд, авторефератa и публикациите са достатъчни за изясняване на получените научни, научно-приложни и приложни резултати.

Авторефератът на дисертационния труд адекватно отразява структурата и съдържанието на дисертационния труд.

Личният принос на кандидата в получаването на резултатите в представените за рецензиране трудове е неоспоримо. Не установих плагиатстване и приемам, че трудовете и приносите в него са лично дело на кандидата.

6. БЕЛЕЖКИ И ПРЕПОРЪКИ

Рецензентът не намира съществени научни грешки в представените разработки и публикации, но си позволява да направи няколко критични бележки и препоръки, в по-голямата си част насочени към подобряването на бъдещите изследвания и публикации:

- Допусната е излишна описателност на известни в науката факти и това е попречило да се акцентира върху наличието на оригинални, значими за развитието на науката теоретични резултати или научни обобщения и тяхното прецизно дефиниране в представеното изследване и открояването им от съществуващите решения.
- Не навсякъде е ясно показан авторският принос:
  - Използваните известни научни резултати;
  - Разделителни протоколи или справки за авторство;
- Да се засили активността при ръководство на научни работници и докторанти и установяване на специфична собствена школа в предметната област на научните изследвания.

7. ЗАКЛЮЧЕНИЕ

Изразявам убеждението си, че доц. д-р Борислав Панайотов Стоянов е един високо ерудиран, образован и коректен преподавател, научен работник и изследовател. Общата му оценка, както и конкретната оценка на научните и практически резултати и приноси, ми дават основание за изразя своето положително становище и да предложа на членовете на уважаемото жури да гласуват положително за даване на научната степен **„ДОКТОР НА НАУКИТЕ"** на доц. д-р Борислав Панайотов Стоянов в област на висшето образование

4. Природни науки, математика и информатика към професионално направление 4.6 Информатика и компютърни науки, научна специалност Информатика.

13.05.2015 г. **Член на журито:**

гр. Шумен **/проф. д.т.н. Веселин Целков/**