СТАНОВИЩЕ

от

доц. д.н. Георги Николов Кръстев
факултет „Електротехника, електроника и автоматика"
при Русенски университет

присъждане на научна степен **"доктор на науките"**

Област на висше образование: **4. Природни науки, математика и информатика**
Професионално направление: **4.6. Информатика и компютърни науки**
Факултет: **Математика и информатика**
Катедра: **Компютърна информатика**

Тема на дисертационния труд: **"Криптографски алгоритми за защита на информацията"**
Автор на дисертационния труд: **доц. д-р Борислав Панайотов Стоянов**

Становището е изготвено и представено на основание на заповед РД-16-068/24.04.2015 г. на Ректора на Шуменски Университет „Епископ Константин Преславски", както и на решение на научното жури, взето на неговото първо заседание.

1. Данни за дисертанта

Борислав Панайотов Стоянов е роден през 1976. Завършил е Шуменски Университет „Еп. К. Преславски" през 2000 г. със специалност „Информатика" и през 2006 защитава докторската си дисертация и получава образователна и научна степен „доктор". През 2009 г. му е присъдено званието „Доцент" в Шуменски Университет „Еп. К. Преславски".

2. Данни за докторантурата

Във връзка със задълженията от Правилника за условията и реда за придобиване на научни степени и заемане на академични длъжности (УРПНСЗАД) в Шуменски Университет „Еп. К. Преславски" и в съответствие с изискванията на чл.41 от Правилника за УРПНС, научното жури не е констатирало несъответствия и нарушения на нормативните изисквания във връзка с докторантурата.

3. Данни за дисертацията и автореферата

Дисертационния труд е с общ обем от 187 страници и е структуриран в увод, четири глави, заключение, списък на

съкращенията, декларация за оригиналност, библиография, публикации по дисертационния труд и списък на известни цитирания по темата.

В увода е дефинирана основната цел на дисертационната работа и задачите за постигането ѝ.

В първа глава е представен обектът за изследване. Разкрити са основните компоненти на криптографската система. Изяснен е проблемът за същността на генерирането на псевдослучайни двоични редици. Представени са основните свойства, които трябва да притежават псевдослучайните двоични редици. Приведени са структурите и основните характеристики на линейните преместващи регистри с обратна връзка и преместващите регистри с обратна връзка и пренос. Изследвани са следните криптографски алгоритми:

- Сумиращ генератор, изпълнен с N-преместващи регистри с обратна връзка и пренос с различна адичност;
- Метод за синтезиране на перфектни двумерни масиви;
- Алгоритъм за обработка на сигнали без загуба на информация;
- Сумиращ-свиващ p-адичен псевдослучаен генератор.

Във втора глава е синтезиран модифициран самосвиващ генератор, изпълнен с преместващ регистър с обратна връзка и пренос, и предложената схема притежава подходящите свойства за различни криптографски модули. Софтуерно е моделиран и статистически изследван модифициран самосвиващ генератор, изпълнен с линеен преместващ регистър с обратна връзка. Предложен и изследван е нов модифициран самосвиващ генератор, изпълнен с преместващ регистър с обратна връзка и пренос, както и със свиващата функция на Jabri. Синтезиран е редактиращ битове-търсещ генератор, базиран на преместващ регистър с обратна връзка и пренос. Извършено е експериментално паралелно криптиране с редактиращия битове-търсещ генератор, базиран на преместващ регистър с обратна връзка и пренос. Моделирано и изследвано е филтриране на преместващ регистър с обратна връзка и пренос чрез бент булева функция.

В трета глава е синтезиран и изследван псевдослучаен генератор на битове, базиран на стандартното кръгово изображение. Разработен е псевдослучаен генератор на битове на основата на стандартното изображение на Chirikov, филтрирано чрез свиващото правило на Jabri. Моделиран и изследван е псевдослучаен генератор, базиран на изображението на Tinkerbell. Синтезиран е псевдослучаен генератор, базиран на изображението на Zaslavsky. Моделиран е модифициран псевдослучаен генератор, базиран на изображението на Chebyshev. Синтезиран е псевдослучаен генератор на основата на изображението на Duffing. Моделиран и изследване е псевдослучаен генератор, базиран на атрактора на Lorenz, филтриран чрез бент булева функция. Проведено е експериментално тестване, показващо пълно преминаване на приложените статистически тестове.

В четвърта глава е разработена и изследвана схема за защита на изображения чрез преместващ регистър с обратна връзка и пренос филтриран чрез функцията на Jabri. Моделирана е схема за защита на изображения чрез атрактора на Lorenz и е синтезирана схема за защита на изображения чрез изображението на Duffing и изображението на Chebyshev. На базата на теоретичните и експериментални изследвания е направен извод, че предложените алгоритми са подходящи за практическа защита на изображения.

Авторефератът на дисертацията представя и отразява точно и стегнато основните положения, резултатите и приносите на дисертационния труд.

4. Научни,научно-приложни и приложни приноси

Най-общо приемам класификацията на автора на приносите в дисертационния труд като научни, научно-приложни и приложни.

Научните приноси са свързани с направената класификация на криптографските алгоритми за поточно шифриране, както и предложения теоретичен подход за синтез на криптографски алгоритми за защита на информацията в различни направления.

Научно-приложните приноси в дисертацията включват разработените и/или изследвани алгоритми в областта на: псевдослучайни криптиращи алгоритми чрез преместващи регистри с обратна връзка; повишаване скритостта на комуникационните системи; синтезирането на криптографски алгоритми за генериране на псевдослучайни двоични редици чрез нелинейни динамични системи и моделиране на криптографски алгоритми за защита на изображения.

Приложните приноси в дисертацията са свързани с въвеждане и прилагане на предложените модели и алгоритми за редица практически задачи.

5. Преценка на публикациите по дисертационния труд

Публикациите на дисертанта са двадесет и седем, като осем са самостоятелни. В рецензирани издания са деветнадесет. Деветнадесет са на латиница и осем - на български. Представена е справка за импакт фактор на списанията, в които са публикациите, свързани с дисертацията.

Представени са 37 цитирания на латиница и повечето са в чужбина. Това свидетелства, че резултатите от изследванията са намерили публичност сред научната общност.

6. Мнения, препоръки и бележки

Целта и задачите на дисертационната работа са споменати в увода, но те не са изведени въз основа на критичен анализ на проблемите, свързани със създаването и изследването на криптографски алгоритми

за защита на информацията. Би трябвало такъв анализ да бъде направен в първа глава и на база на изводите от този анализ да бъде обоснована целта и съответните задачи на дисертацията.

Липсва обобщен анализ на проблемите, разглеждани в дисертацията. Различните проблеми са формулирани в отделните глави и там са предлагани подходите за решаването им.

Удачно би било още в началото на всяка от главите на дисертационния труд да бъдат дадени, кои от публикациите по дисертацията третират проблемите в съответната глава. По този начин по-ясно ще бъде подчертано разпределението на публикациите по глави.

На някои места в ръкописа има стилови неточности, по-трудно разбираеми текстове и т.н., което е неизбежно при големия обем информация, която е представена в дисертационната работа.

Бих си позволил да препоръчам на автора да формира по-широк колектив от опитни, а също така и млади учени и докторанти, с цел доразвиване на идеите от дисертацията в следващи научни изследвания и участие в международни проекти.

7. Заключение

По начина на разработване, структура и обем, по съдържание и постигнати резултати, представеният дисертационен труд отговаря на изискванията на Закона за развитие на академичния състав в Република България, Правилника за неговото прилагане и Правилника за условията и реда за придобиване на научни степени и заемане на академични длъжности в Шуменски Университет „Епископ Константин Преславски", което е основание да предложа на научното жури да присъди на доц. д-р Борислав Панайотов Стоянов научната степен "ДОКТОР НА НАУКИТЕ".

27.05.2015 г.
гр. Русе

Член на журито:
/ доц. д.н. Г. Кръстев