ШУМЕНСКИ УНИВЕРСИТЕТ
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

Р Е Ц Е Н З И Я

от професор д.т.н. Атанас Иванов Начев, домашен адрес:
гр. София, бул.” Мария Луиза № 67, вх. “Б”,
тел. (02)983 96 81, GSM 0888/49 87 02.

Относно: дисертационен труд за присъждане на научна степен “доктор на науките” на **тема:** „Криптографски алгоритми за защита на информацията”, с **автор** доц. д-р Борислав Панайотов Стоянов.

Шумен
2015

I. Документи

Като рецензент са ми представени следните документи:

1.1. Ръкопис на 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.

2.2. Автореферат на дисертационния труд.

II. Кратка оценка на представената документация

Представените ми документи, по обем и съдържание, са достатъчни за изясняване на получените в резултат на дисертационното изследване научни, научноприложни и приложни резултати.

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

III. Актуалност на дисертационния труд

Докторантът формулира основната си цел като: „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“.

Така дефинираната основна цел на дисертационното изследване се доуточнява чрез задачите, които са решени, а именно:

1. Изследване и разработване на криптографски алгоритми за генериране на псевдослучайни числа на основата на преместващи регистри с обратна връзка.

2. Изследване и разработване на криптографски алгоритми за генериране на псевдослучайни числа чрез нелинейни динамични системи.

3. Изследване и разработване на криптографски алгоритми за защита на изображения.

Тези изследвания имат отношение към решаване на проблеми, свързани със защитата на информацията в компютърните и комуникационни системи и мрежи. Това е, актуално и нужно направление за научни изследвания. То пряко комуникира със съвременните тенденции в науката и има непосредствено приложение в техниката .

IV. Описание на труда

Представения ми за рецензия ръкопис е структуриран в увод, четири глави, заключение и списък с използваната литература.

Уводът е структуриран и изпълнен по начин, който позволява да се получи представа за характера и съдържанието на дисертационното изследване.

Глава първа е встъпителна. В нея авторът развива своето виждане за състоянието на нещата, развитието им и проблемите, отнасящи се до генериране на псевдослучайни двоични последователности чрез регистри с обратна връзка. Той подлага на сериозен анализ използването за целта на преместващи регистри с обратна връзка, моделирането на сумиращи псевдослучайни генератори чрез преместващи регистри и моделирането на свиващи псевдослучайни генератори чрез преместващи регистри. На базата на това са дефинирани основни свойства, които следва да притежават псевдослучайните двоични редици. Това се допълва с резултатите от изследването на основни, използвани в теорията и практиката криптографски алгоритми.

Изложеното **във втора глава** е свързано с генериране на самосвиващи псевдослучайни битови последователности чрез преместващи регистри с обратна връзка. Синтезиран е самосвиващ 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.

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

В **трета глава** вниманието на автора е насочено към генериране на псевдослучайни последователности с използване на нелинейни динамични системи. В тази връзка са разработени: 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; 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.

Четвърта глава е посветена на защитата на изображения посредством криптографски алгоритми. За целта са разработени: метод за защита на изображения чрез преместващ регистър с обратна връзка и пренос, филтриран чрез функцията на Jabri и метод за защита на изображения посредством изображенията на Duffing и Chebyshev.

Предложените методи за защита на изображения са изследвани и е доказана тяхната ефективност им чрез разработени за целта математически модели.

V. Аналитична характеристика на дисертационния труд

Прави впечатление теоритикоприложния характер на дисертационния труд, определен от постановката на задачата и от начините на формализиране и търсене на решения. В нея се разглежда спецификата на проблемите, свързани с разработване на криптографски алгоритми за защита на информацията. Предлагането на нови решения за постигане на целта на дисертационното изследване затвърдява представата за неговата завършеност и приложимост на получените резултати за нуждите на теорията и на практиката.

VI. Научни приноси

Като научен принос с методичен характер рецензентът приема приетия подход за решаване на проблемите, свързани с разработване и изследване на нови криптографски алгоритми за защита на информацията, в това число:

1. Сумиращ генератор, изпълнен с N-преместващи регистри с обратна връзка и пренос с различна адитичност.
2. Самосвиващ генератор, реализиран посредством преместващ регистър с обратна връзка и пренос.
3. Самосвиващ генератор, изпълнен с 2-адичен преместващ регистър с обратна връзка и пренос, с използване на свиваща функция на Jabri.
4. Самосвиващ псевдослучаен генератор, реализиран с използване на p-преместващ регистър с обратна връзка и пренос.
5. Псевдослучаен генератор на битове, базиран на стандартно кръгово изображение.
6. Псевдослучаен генератор на ботове, базиран на стандартно изображение на Chirikov, филтрирано посреством свиващо правило на Jabri.
7. Псевдослучаен генератор, базиран на изображение на Zaslavski.
8. Псевдослучаен генератор, базиран на изображение на Chebyshev.

9. Псевдослучаен генератор, базиран на изображение на Duffing.

10. Защита на изображение чрез прилагане на изображението на Chebyshev и на изображението на Duffing.

11. Разработените математически модели за доказване на ефективността на предлаганите методи и алгоритми, в целия текст на дисертационния ръкопис.

VII. Научноприложни и приложни приноси

Получените резултати от дисертационното изследване, които показват приложимостта и съдържателността им в пълния обем на ръкописа на дисертацията.

VIII. Относно публикациите на докторанта

Рецензентът никога не е придавал кой знае какво значение на формалната оценка на представянето в печата на едни или други резултати от дадено изследване, във всеки случай не повече отколкото дадено издание заслужава. За него е от значение не къде е публикуван дадения материал, а какво е неговото съдържание от гледна точка на новостите в науката.

Като изхожда от казаното, и предвид на съдържателната част на публикациите рецензентът приема публикационната дейност на докторанта за съответстваща, по своето съдържание, на изискванията за получаване на научната степен „доктор на науките".

VIII. Забележки по дисертационния ръкопис

Основно изискване за получаване на научна степен „Доктор на науките" е наличието на оргинални, значими за развитието на науката теоретични резултати или научни обобщения. Такива в предлагания дисертационен труд безспорно присъстват. За съжаление авторът на дисертационното изследване не ги е дефинирал в достатъчно ясенен вид в дисертационния ръкопис. Излишната описателност на известни неща също не допринася за строгостта на изложението.

XI. Изводи от бележките

Посочените забележки са пропуски. Отнасят се до прозрачността и строгостта на изложението. Те в никаква степен не поставят под съмнение избрания подход при организирането и провеждането на научните изследвания, използвания за целта инструментариум и неговото прилагане, а така също и интерпретацията на получените в хода на научното търсене резултати.

ЗАКЛЮЧЕНИЕ:

На основание на изискванията на "Закона за развитието на академичния състав в Република България" и на Правилника за неговото прилагане и като вземам под внимание казаното в пълния

обем на настоящата рецензия, оценявам положително дисертационния труд на тема " Криптографски алгоритми за защита на информацията" и ще гласувам положително на автора му доц. д-р Борислав Панайотов Стоянов да се присъди научната степен „доктор на науките".

РЕЦЕНЗЕНТ:

ПРОФЕСОР АТАНАС НАЧЕВ,
ДОКТОР НА ТЕХНИЧЕСКИТЕ НАУКИ

11 май 2015 г.
гр. Шумен