KONSTANTIN
PRESLAVSKY
UNIVERSITY
SHUMEN

ШУМЕНСКИ УНИВЕРСИТЕТ
"ЕПИСКОП КОНСТАНТИН
ПРЕСЛАВСКИ"

ФАКУЛТЕТ ПО ТЕХНИЧЕСКИ НАУКИ
КАТЕДРА "КОМУНИКАЦИОННА И КОМПЮТЪРНА ТЕХНИКА"

С Т А Н О В И Щ Е

от проф. д-р инж. Иван Кръстев Цонев – катедра „Комуникационна и компютърна техника на Факултета по технически науки в Шуменски университет „Е. К. Преславски"

на тема

" КРИПТОГРАФСКИ АЛГОРИТМИ ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА"

за присъждане на образователната и научна степен „доктор на науките" в научна област: 4 Природни науки, математика и информатика, професионално направление: 4.6 Информатика и компютърни науки, научна специалност: Информатика

Разработена от доц. д-р Борислав Панайотов Стоянов

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

Дисертационният труд е в обем от 187 стр. и съдържа увод , четири глави и заключение. Трудът съдържа 65 таблици и 29 фигури. Цитирани са 188 литературни източника, от които 33 на кирилица и 155 на латиница.

Обект на изследване в дисертационния труд са псевдослучайните генератори на редици, алгоритмите за защита на изображения на основата на хаотични функции и криптографските алгоритми за повишаване на комуникационната сигурност. Изследвани са аналитичните свойства и криптоустойчивостта на псевдослучайни генератори на битове и алгоритмите за защита на графични изображения.

Направена е обосновка на криптографската защита на съобщения чрез използване на генератори на псевдослучайни двоични последователности (ПСП) от преместващи регистри с обратна връзка. Разработени са модели на сумиращ псевдослучаен генератор с използване на преместващи регистри. Анализирани са алгоритми за синтез на двумерни масиви и обработка на сигнали без загуби. Приложени са бент булеви функции в обратната връзка на генератор на ПСП. Предложено е генериране на ПСП чрез използване на нелинейни динамични системи. Разработена е защита на изображения чрез използване на криптографски алгоритми.

2. Актуалност на проблема

Актуалността на предметната област е обоснована от необходимостта за ефективно противопоставяне срещу заплахи за личната, институционална и фирмена сигурност. Криптографските алгоритми са важен компонент във всички комуникационни и информационни системи. Поради тези причини синтезирането и изследването на нови модели и алгоритми в областта е актуален научен проблем. Доц. д-р Панайотов е провел в областта изследвания в четири основни направления: генериране на псевдослучайни последователности чрез преместващи регистри с обратна връзка и пренос, синтез на псевдослучайни последователности чрез хаотични функции, защита на изображения чрез преместващи редици с обратна връзка и пренос с използване на хаотични функции, генериране на криптографски алгоритми за повишаване на комуникационната сигурност.

Целта на дисертационния труд е изследване и разработване на нови модели и криптографски алгоритми за защита на съобщенията чрез използване на различни преместващи регистри с обратна връзка.

За постигане на целта авторът си е поставил за решаване на три основни задачи:

1. Да се разработят и изследват криптографски алгоритми за генериране на псевдослучайни числа на основата на преместващи регистри с обратна връзка.
2. Да се разработят и изследват криптографски алгоритми за генериране на псевдослучайни числа чрез нелинейни динамични системи.
3. Да се разработят и изследват криптографски алгоритми за защита на изображения.

Целта и задачите на дисертационния труд са формулирани коректно и изпълнени в пълен обем.

3. Приноси на дисертационния труд

В резултат на проведените изследвания в представения дисертационен труд са получени теоретични и приложни приноси от значение за защитата на информацията в комуникационните и информационни системи.

- Синтезирани са криптографски алгоритми използващи генериране на псевдослучайни последователности с помощта на преместващи регистри с модифицирана обратна връзка;
- Изследвани са криптографски алгоритми за ефективно скриване на съобщенията в комуникационните системи;
- Синтезирани са на криптографски алгоритми за генериране на псевдослучайни двоични редици чрез нелинейни динамични системи и са изследвани осем криптографски алгоритъма;
- Изследвани са модели на криптографски алгоритми за защита на изображения.

Нямам съмнение, че дисертационния труд е лично дело на докторанта. Получените резултати са представени в публикации на авторитетни научни форуми в страната и чужбина. Доц. д-р Панайтов е направил и декларация за оригиналност на получените приноси.

По дисертационния труд са направени 27 публикации в авторитетни научни форуми и списания в страната и чужбина. Цитирани са 15 труда, от които един е цитиран 6 пъти, четири са цитирани 4 пъти, три са цитирани 3 път, четири са цитирани 2 пъти и три са цитирани 1 път. По-голяма част от цитатите са направени в издания с импакт фактор.

4. Критични бележки и препоръки по дисертацията

Някои елементи от структурата на дисертационния труд са представени подробно и описателно, с което се отклонява вниманието от същността на постигнатите резултати. Изводите след всяка глава и получените приноси са представени без да се акцентира върху получените новости в развитието на фундаменталната теория.

Препоръчвам на доц. д-р Панайотов да усъвършенства стила на изложение при представянето на теоретични изводи и обобщения.

5. Заключение

Постигнатите наукометрични резултати от доц. д-р Панайотов напълно съответстват на приетите изисквания за научна степен „доктор на науките“ в Шуменски университет „Е. К. Преславски“ и Факултета по математика и информатика. Дисертацията, авторефератът и публикуваните трудове към тях от кандидата отговарят на изискванията на ЗРАСРБ за получаване на научната степен „доктор на науките“, което ми дава основание да направя обобщение, че доц. Д-р Панайотов е водещ учен и педагог в областта на математиката и информатиката, провел е задълбочени научи изследвания, получени са научно-приложни и приложни резултати от значение за фундаменталната теорията и практиката в информатиката. Резултатите от научните му изследвания са публикувани в авторитетни научни форуми и списания в страната и чужбина.

Получените приноси в дисертационния труд са основание за положителна оценка и предлагам на членовете на научното жури и да се присъди научна степен "доктор на науките" в научна област: 4 Природни науки, математика и информатика, професионално направление: 4.6 Информатика и компютърни науки, научна специалност: Информатика.

25.05.2015 г.

Автор:.....

/Проф. д-р И. Цонев/