МИНИСТЕРСТВО НА ОТБРАНАТА
ИНСТИТУТ ПО ОТБРАНА „ПРОФЕСОР ЦВЕТАН ЛАЗАРОВ”
София 1592, бул. „Проф. Цветан Лазаров” № 2, факс: 02/92 21 808, http://di.mod.bg

РЕЦЕНЗИЯ

от доц. д-р **Александър Асенов Колев**,

член на научното жури на дисертационния труд на
инж. **Андрей Георгиев Иванов**

на тема „АНАЛИЗ НА УСТОЙЧИВОСТТА НА КРИПТОГРАФСКИ СИСТЕМИ С ПУБЛИЧЕН КЛЮЧ”

за придобиване на образователна и научна степен „доктор” по докторска програма „Автоматизирани системи за обработка на информация и управление“, професионално направление 5.2 „Електротехника, електроника и автоматика“, област на висшето образование 5. „Технически науки“

1. Актуалност и значимост на разработвания научен проблем

Използването на криптография с цел защита на чувствителна информация от държавно, военно и лично значение е известно и широко прилагано още от древността. Технологичното развитие и напредъка в информационната и комуникационна сфери в нашето съвремие съществено разшири обхвата и повиши необходимостта от ползване на криптография, достигайки практически до всеки човек с необходимост от защитено подаване на лични данни по електронен път. Така говорим за публична криптография, за която може да се твърди, че е в основата на функционирането на съвременното общество, държавите и световните процеси.

Криптографските системи за защита на информацията, основана на известия подход за ползване на публичен ключ са от голяма практическа важност. Актуалността и значимостта на дисертационния труд проличава в поставената цел и задачи, отнасящи се до определяне на степента на устойчивост при функционирането на криптографски системи с публичен ключ. Несъмнено е съответствието на темата на дисертационния труд с основното съдържание на представения за рецензиране текст. В работата си инж. Андрей Иванов разглежда и анализира най-широко прилаганите в практиката алгоритми и подходи, използвани в публичната криптография с цел защита на информация и оценява степента на тяхната устойчивост на атаки, свързани с наличието на определени слабости. Като новост определям част от изследователската работа, свързана с установяването на преднамерено създадени криптографски уязвимости, известни под общо наименование „клептография“. Авторът разработва модели, чрез които може да се определи вероятност за съществуването или не съществуването на уязвимости от такъв „клептографски“ вид.

2. Обща характеристика и структура на дисертационния труд

Дисертационният труд се състои общо от 144 страници, от които 106 страници основна част и 21 страници приложение. В основната част на дисертацията са приложени 10 фигури и 25 описани алгоритъма във вид на псевдокод. При работата си по дисертационния труд, авторът е ползвал 114 цитирани литературни източници.

Дисертационният труд е структуриран в стандартен формат, състоящ се от въведение, три глави, заключение, литература, списък на направените публикации при разработка дисертацията, списък на използваните термини, математически означения и основни функции, списък на фигурите.

В първа глава са разгледани математически и алгоритмични основи на публичната криптография, описана е тяхната приложност и сфери на използване, прилагани в практиката стандарти и изисквания към системите, използващи публичната криптография. Оценени са проблемите, свързани с устойчивостта на функциониране на криптографски системи с публична криптография и са формулирани целта и задачите на разработвания научно-изследователски труд.

Във втора глава са предложени два модела на решение на поставените проблеми. Първият модел на решение е построен с предназначение за постигане на по-голяма ефективност и достоверност на резултата за определяне делимост на число, чрез използване на вероятностният алгоритъм на Милър-Рабин. Вторият модел на решение е предназначен за определяне на математическата възможност за по-ефективно изпълнение на алгоритъма на Силвър-Похлиг-Хелман, чрез който се реализират атаки към най-разпространения в практиката към настоящия момент криптографски алгоритъм в публичната криптография, известен с абревиатурата RSA и разработен от колектива на Ron Rivest, Adi Shamir и Leonard Adleman.

В трета глава са описани математическите основи и модел на нов (предложен от автора) подход за реализация на алгоритъм за клептографски цели. Направен е сравнителен анализ между предлагания алгоритъм и други съществуващи клептографски алгоритми. Направен анализ и е извършена оценка за възможността за съществуване и използване на клептография в практически-приложни системи, базирани на публична криптография. Предложен е механизъм, чрез който да се избегнат уязвимости, отнасящи се до клептографски атаки към системи, базирани на RSA. Приведени са резултати от тестовете, постигнати с прилагане на създадено софтуерно приложение за генериране на ключове за RSA, с ползване на предложения клептографски алгоритъм.

Внимателното запознаване с представения за рецензиране дисертационен труд дава представа за високото качество на извършената от автора научно-изследователска работа. Систематично и последователно могат да се проследят елементи на прилагана методика за научни изследвания във вида: анализ на научно-практически проблем, поставяне на научна хипотеза, синтез на модел на решение, експериментално потвърждаване на очакваните резултати с провеждане на софтуерен експеримент.

3. Характеристика на научните и научно-приложните приноси в дисертационния труд. Достоверност на материала

Приносите на инж. Андрей Иванов могат да се определят като научно-приложни и приложни. Приемам посочените в текста на дисертацията труд приноси, които са:

- Предложен е модел на решение, позволяващ повишаване на достоверността на резултата за оценка делимост на число като допълнение към известния алгоритъм на Милър-Рабин. Предложеният модел на

решение е апробиран с проиграване на два числени примера, представени в Приложение 1;

- Предложен е нов модел за решаване на системи от конгруентни уравнения, без изпълнимостта на модела да зависи от съществуващи ограничаващи условия. Моделът позволява постигане на решения без да е необходимо числата, с които се изчислява по модул да са взаимно прости. Използването този модел в допълнение към алгоритъма за атака на RSA, предложен от Похлиг-Хелман повишава бързодействието на неговото изпълнение. В подкрепа на предложеният нов модел за решаване на системи от конгруентни уравнения е проигран числов пример, Приложение 2;

- Представен е математически апарат и практическо решение, което позволява създаването на клептографски алгоритъм за атака на RSA базирани криптографски системи. Направен е сравнителен анализи и оценка как клептографски алгоритми от този тип застрашават устойчивостта на функциониране на системи, използващи RSA. Тези резултати повдигат въпрос към достатъчността на условията в състава на сега прилаганите стандарти за оценка на качеството на генериран RSA ключ. Действието на представения математически апарат и практическото решение са онагледени в числов вид в Приложения 3, 4 и 5.

4. Оценка на научните резултати и приносите на дисертационния труд

Научно-приложните и приложни приноси в дисертационния труд определям като обогатяване на съществуващи знания със значителен по стойност ефект при едно бъдещо широко практическо прилагане. Проведеният в т. 3.3 от дисертационния труд „Сравнителен анализ и оценка на възможността за откриване“ на вградени клептографски

механизми в прилагани криптографски системи определям като съществено научно-практическо приложение.

В полза на поставената висока оценка на получените дотук резултати говорят набелязаните цели за разширяване на научно-изследователската работа по тематиката на настоящата дисертация, които могат да се обобщят като:

- Повишаване на устойчивостта и надеждността на генериране на ключове, използвани в публичната криптография;
- Качествена и бърза оценка за наличие на внедрена клептография в системи, използващи публична криптография;
- Създаване на модели, които да послужат като алгоритмична основа за бъдещи високопроизводителни хардуерни криптографски решения.

Включените в дисертационния труд резултати с предшестваща научна обосновка, както и цялостното хармонично впечатление от структурата на материала са основа на увереността ми, че работата е лично дело на инж. Андрей Иванов.

5. Оценка на публикациите по дисертацията и авторството

В приложения към дисертационния труд „Списък на свързаните с дисертацията публикации“ са посочени три заглавия. В две от тях инж. Андрей Иванов фигурира като първи автор, което говори за неговото преимуществено участие в подготовката на публикациите. Една от публикациите на английски език е в международното специализирано издание на Springer, Communications in Computer and Information Science, друга публикация, също на английски език е в международното специализирано издание Information & Security: An International Journal. Останалата посочена в списъка публикация на български език е в материалите на международна научна конференция „Научните

изследвания и инвестициите в технологични иновации – решаващ фактор за отбраната и сигурността“.

Всички публикации съответстват на темата на дисертационния труд. Без да има приложен списък на цитиранията, в публичното пространство могат да се проследят две цитирания на публикации от списъка.

6. Литературна осведоменост и компетентност на докторанта

При работата си по дисертационния труд инж. Андрей Иванов е ползвал 114 литературни източника. От тях 79 източника са публикации в специализирани научни издания и материали от научни форуми. Останалите 35 цитирани позиции са електронни източници и ресурси. Два от литературните източника са на български език, останалите са англоезични.

Всички посочени литературни източници намират своето отражение в основния текст на дисертационния труд и са подходящо ползвани в подкрепа на защитаваната от автора теза. Свободното боравене с подобен богат по количество и качество научен материал показва много добрите познания на автора по тематиката на разработения от него дисертационен труд.

7. Оценка за автореферата

Представеният автореферат на дисертационния труд се състои от 40 страници на български език. В автореферата са показани съществените моменти от трите глави на труда, заключение, постигнати резултати и списък на свързаните с дисертацията публикации.

Авторефератът съответства на изискванията на Закона за развитие на академичния състав в Република България (ЗРАСРБ).

8. Критични бележки

Отправям следните критични бележки към оформлението на дисертационния труд:

• Фигура 2, поместена в текста на т. 1.1.2 е с неподходяща резолюция, което затруднява възприемането на представеното в нея графично съдържание;

• Списъкът с цитираните електронни източници и ресурси не е оформен в типичния за подобни материали формат. За някои от електронните източници не е посочен момента във времето, когато са били достъпвани.

Посочените от мен критични бележки в никакъв случай не се отразяват на високото качество като цяло на рецензирания дисертационен труд.

Към инж. Андрей Иванов отправям препоръката в бъдеще да насочва повече свои публикации към издания, които са индексирани в международно признати бази от данни с научна продукция.

9. Лични впечатления

По приложените автобиографични данни инж. Андрей Иванов през 2000 г. завършва висшето си образование във ВВУАПВО „Панайот Волов“, специалност „Изчислителна Техника и АСУВ“ с образователно-квалификационна степен магистър. Работи като военнослужещ в системата на Министерство на отбраната до 2019 г., когато се уволнява от военна служба и преминава в редовете на военния резерв. След 2019 г. работи в IT компании, чиято дейност е свързана с криптография и киберсигурност.

Познавам инж. Андрей Иванов от лични срещи по време на участия в научни форуми, както и при посещенията му през последните няколко години в Институт по отбрана „Професор Цветан Лазаров“. По време на

проведени с него разговори на научна тематика и по въпроси, свързани с работата му по настоящия дисертационен труд, той показва високо ниво на научна подготовка и компетентност в сферата на провежданите от него научни изследвания.

Смятам, че инж. Андрей Иванов притежава голям потенциал за развитие като млад учен в избраното професионално направление.

10. Заключение

В следствие на посоченото дотук, определям дисертационния труд на инж. Андрей Иванов като отговарящ на изискванията на „Правилник за условията и реда на придобиване на научни степени в Институт по отбрана“ и ЗРАСРБ за придобиване на образователната и научна степен „доктор”.

11. Оценка на дисертационния труд

Давам положителна оценка на дисертационния труд и приложенията към него. Препоръчвам на уважаемите членове на Научното жури и на уважаемите членове на Научния съвет да гласуват **ЗА** присъждането на инж. **Андрей Георгиев Иванов** на образователна и научна степен „доктор“ по докторска програма „Автоматизирани системи за обработка на информация и управление“, професионално направление 5.2 „Електротехника, електроника и автоматика“, област на висшето образование 5. „Технически науки“.

Дата: 07.02.2022 г.

Рецензент: ...../П/.....

(доц. д-р Александър Колев)