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

СТАНОВИЩЕ

от проф. д-р Росен Станков Илиев,
Институт по отбрана „Професор Цветан Лазаров",
София, 1592, бул. „Професор Цветан Лазаров", № 2, тел. 02 92 21821,

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"

Научен ръководител: **полк. доц. д-р Николай Тодоров Стоянов**

1. Актуалност и значимост на разработвания научен проблем

Дисертационният труд разглежда актуален проблем, свързан с прилаганите в практиката алгоритми и подходи на публичната криптография, оценка на степента на тяхната устойчивост на атаки и степента на уязвимости. От формулираната в дисертацията цел е видно, че се търсят да се предложат модели на решение за проверка устойчивостта на функциониране на криптографски системи базирани на алгоритъма за криптиране RSA.

Дисертационният труд е структуриран в увод, три глави, заключение, литература, списък на публикации, свързани с дисертацията, списък на използваните термини, математически означения и основни функции, списък на фигурите, в общ обем от 144 стр., с приложенията. Посочената библиография е от 114 източници, предимно на английски език от областта на дисертационния труд. Списъкът на свързаните с дисертацията публикации включва три съвместни с научния му ръководител публикации, една от които е в издание Springer.

Съдържанието на дисертационния труд съответства напълно на темата на дисертацията. То представлява едно полезно изследване на математически и алгоритмични основи на публичната криптография с предложение на два модела за постигане на по-голяма ефективност и достоверност на резултата при определяне на делимост на число при използване на вероятностния алгоритъм на Милър-Рабин, както и за по-ефективно изпълнение на алгоритъма на Силвър-Похлиг-Хелман, чрез който се реализират атаки към най-разпространения в практиката криптографски алгоритъм в публичната криптография. Представеният модел на решение за определяне делимост на числа, дава възможност за подобряване оценката на генерираните ключове за криптографски системи базирани на RSA.

2. Оценка на научните резултати и приносите на дисертационния труд

Дисертационният труд на инж. Андрей Иванов е разработен в необходимия обем и пълнота, а от неговото съдържание личи, че авторът много добре е запознат с проблемната област и с възможностите за решаване на поставените изследователски задачи. Формулираните резултати в дисертацията са логично следствие от извършените научни и приложни изследвания, включващи необходимите модели и математически апарат за тяхното описание. Интерес представлява предоженият подход за създаване на клептографски алгоритъм с описание на неговата практическа реализация, генериране на домейни за публичен ключ и представената проверка на постигнатите резултати чрез сравнителен анализ с други съществуващи клептографски алгоритми. Предложен е също така математически апарат и практическо решение за създаването на клептографски алгоритъм за атака на RSA базирани криптографски системи.

Приемам дефинираните от автора резултати като развитие и обогатяване на съществуващите знания и приложение на научните достижения за решаване на важни практически задачи, свързани с повишаване защитата на информацията и устойчивостта на криптографски системи с публичен ключ. Считам, че дисертационният труд и получените в него резултати са лично дело на инж. Андрей Иванов и са следствие от високата му теоретична подготовка, както и от активната му дейност при провеждане на съответните научни изследвания и практически реализации.

Не съм забелязал наличие на плагиатство в работата на автора. Стилът на изложение и логическата последователност на изказа му ми дават увереност за безспорно лично участие на инж. Андрей Иванов в приносната част на дисертацията.

Авторефератът съответства на дисертационния труд и адекватно отразява постигнатите от автора резултати.

3. Критични бележки

Нямам съществени критични бележки по дисертационния труд и автореферата. Запознат съм с първоначалния вариант на дисертацията представен на предварителната защита и с радост констатирам, че голяма част от направените забележки са отстранени, а мои и на колегите ми препоръки са взети под внимание. Въпреки, че постигнатите резултати е можело да бъдат по-ясно формулирани, това по никакъв начин не намалява качеството на представения дисертационен труд.

Препоръчвам на автора да продължи по-нататъшната си работа по възникналите с написването на дисертацията идеи и да насочи бъдещите си изследвания в по-конкретни практически реализации, като резултатите от тях да публикува в престижни научни издания.

4. Заключение

Познавам инж. Андрей Иванов като докторант в Института по отбрана. Личните ми впечатления са, че той е много добър и последователен изследовател, с богат професионален опит в областта на криптографията и защитата на информацията, проявяващ голямо усърдие и собствен стил при првеждане на научните изследвания в областта на неговите научни интереси.

Разработеният дисертационен труд на инж. Андрей Иванов е едно завършено научно изследване по актуален и важен проблем и по съдържание, обем и структура напълно отговаря на изискванията, предвидени в Закона за развитие на академичния състав на Република България (ЗРАСРБ) за присъждане на образователна и научна степен „доктор".

5. Оценка на дисертационния труд

От съдържанието на дисертацията, автореферата, изпълнението на процедурните изисквания по спазването на ЗРАСРБ, както и моите лични впечатления, ми дава основание да дам ПОЛОЖИТЕЛНА ОЦЕНКА на дисертациония труд „Анализ на устойчивостта на криптографски системи с

публичен ключ" и предлагам на автора, Андрей Георгиев Иванов, да се присъди образователна и научна степен „доктор", в област на висшето образование 5 „Технически науки", професионално направление 5.2 „Електортехника, електроника и автоматика".

Член на журито: ...../П/.....

Дата: 08.02.2022 г. (проф. д-р Росен Илиев)