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 **проф. д.т.н. ВЕСЕЛИН ЦЕЛКОВ**

УНИВЕРСИТЕТ ПО БИБЛИОТЕКОЗНАНИЕ И ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

на дисертационен труд за присъждане на
образователна и научна степен **„доктор"**

на тема: ***„Анализ на устойчивостта на криптографски системи с публичен ключ"***

докторант: ***инж. Андрей Георгиев Иванов***

област на висшето образование ***5. Технически науки***, професионално направление ***5.2 Електротехника, електроника и автоматика***, научна специалност ***Автоматизирани системи за обработка на информация и управление***

I. АКТУАЛНОСТ И ЗНАЧИМОСТ НА РАЗРАБОТВАНИЯ НАУЧЕН ПРОБЛЕМ

Актуалност

Актуалността на представения дисертационен се определя от широкото разпространение на Интернет, възприемането на информацията като критичен ресурс и нарастващите заплахи за информационната сигурност. В процеса на тоталното разпространение на Интернет въпросите за защита на информационните ресурси и използването на криптографски алгоритми, механизми и услуги става изключително актуален.

Актуалността на извършеното изследване се определя от няколко проблема, свързани с реализацията и сигурността на асиметричните криптографски алгоритми, като:

- Намиране на двойки, прости (взаимно прости) големи числа;
- Разлагане на голямо число на прости множители;
- Как, знаейки публичния ключ, може да се направи обосновано предположение (с голяма достоверност или да се намери) личния ключ;
- Възможности за атака на сигурността на алгоритъма, при определени условия.

Значимост

Значимостта на изследването еднозначно се определя от мястото и ролята на предложените в дисертационния труд решения на част от тези задачи. Решаването на тези задачи е важна част от решението на проблема за гарантиране на информационната сигурност, използването на асиметричните криптографски алгоритми и преодоляването на този проблем има съществено значение за работещите в това направление специалисти. Решение на част от поставените проблеми са представени в

дисертационното изследване.

Отбелязвам:

1. В основата на най-често срещаните алгоритми с публичен ключ са простите числа и разлагането на число на прости множители. В практиката съществуват множество алгоритми за оценка на делимостта (разлагането) на число на прости множители. Алгоритъмът с най-широко приложение е този на Милър-Рабин (Miller-Rabin), който притежава голямо бързодействие, но в практиката се използва реализация като вероятностен алгоритъм за оценка на делимост. ***Авторът е синтезирал оригинален алгоритъм, базиран на нов модел на решение, модификация (разширение) на алгоритъма на Милър-Рабин. Решението позволява повишаване на вероятността за достоверност на резултата и създава възможност за постигане на детерминистичен резултат без да се намалява бързодействието, което алгоритъма на Милър-Рабин притежава във вариант на изпълнение като вероятностен такъв.***

2. Извършен е анализ и сравнение на най-ефективните алгоритми за разлагане на големи числа на прости множители, с които се реализират атаки на криптографски системи базирани на RSA. Един от алгоритмите използвани в практиката е предложеният от Силвър-Похлиг-Хелман (Silver-Pohlig-Hellman). В част от изпълнението на този алгоритъм е необходимо решаване на система от конгруентни уравнения, чрез използването на един от най-фундаменталните алгоритми в теория на числата „Китайска теорема“. За решаване на система конгруентни уравнения с използването на „Китайска теорема“ има изискване числата за изчисляване по модул да са взаимно прости. ***Андрей Иванов е разработил и е представил нов модел на решение, включващ алгоритъм за решаване на системи конгруентни уравнения, който се изпълнява без ограничаващи условия и може да функционира и да постига решения***

без да е необходимо числата, с които се изчислява по модул да са взаимно прости.

3. Представен е математически модел и практическо решение на клептографски алгоритъм, който използван в практиката сериозно може да повлияе върху устойчивостта и сигурното функциониране на RSA базирани криптографски системи.

II. ОБЩА ХАРАКТЕРИСТИКА И СТРУКТУРА НА ДИСЕРТАЦИОННИЯ ТРУД

За рецензиране са предложени:

- Дисертационен труд – 144 стр.;
- Автореферат – 40 стр,;
- Три публикации.

Съдържанието на представения дисертационен труд е изложено на 144 страници, в т.ч. списък на съкращенията и 10 фигури. То е структурирано като увод, три глави, заключение, постигнати резултати и приложения (4 бр.). Даден е списък на използваните и цитирани в текста информационни източници (114 заглавия, от които 2 на български език, 77 на английски и 35 Интернет адреса). Приложен е списък на публикациите на автора по темата, включващ 3 заглавия.

Всяка глава е обособена част от работата и завършва с изводи, които третират получените резултати. Връзката между главите е осигурена от логиката на изложението и позволява да се придобие цялостна представа за научното изследване.

Анализът на информацията от използваната литература и резултатите от предварителните собствени научни изследвания са позволили на автора точно, ясно и кратко да формулира целта и задачите

на изследването. Последователното решаване на поставените задачи в дисертационния труд предполагат и успешното постигане на поставената цел. Достоверността на получените резултати се потвърждава с резултатите и прилагането им в практиката. Детайлното запознаване с дисертационния труд позволява да се проследят логиката и причинно - следствените връзки на синтеза и анализа, при което не остават с съмнения относно оригиналността и достоверността на представения научен материал.

Използваните в дисертационния труд методи на изследване, в т.ч. планиране на експеримента, проверка на адекватността на разработените математически модели и обработката на данните са добре подбрани и правилно представени. Всичко това гарантира високата степен на достоверност на получените резултати и тяхната правилна интерпретация.

Авторефератът отразява в най-пълна степен получените в изследването резултати.

Представените от кандидата инж. Андрей Иванов дисертационен труд и автореферат са оформени в съответствие с изискванията на закона и правилника и изцяло покриват критериите за получаване на образователната и научна степен доктор.

III. ХАРАКТЕРИСТИНА НА НАУЧНИТЕ И НАУЧНО-ПРИЛОЖНИ ПРИНОСИ

Приносите на кандидата могат да бъдат отнесени към научна специалност ***Автоматизирани системи за обработка на информация и управление*** и в показаните по-горе направления и могат да бъдат обобщени (според рецензента) в областите:

- Методи, подходи, модели и изследвания за повишаване на достоверността на резултата за оценка делимост на число като

допълнение към най-широко прилагания в практиката допълнение към най-широко прилагания в практиката алгоритъм, този на Милър-Рабин;

- Нови модели на решаване на системи конгруентни уравнения, при който не съществуват ограничаващи условия, за да бъде модела изпълним. Липсата на ограничаващи условия го отличава от досега известните в практиката алгоритми, като този на „Китайската теорема“ и позволява постигане на решения без да е необходимо числата, с които се изчислява по модул да са взаимно прости;
- Разработването на математически апарат и практическо решение, което позволява създаването на клептографски алгоритъм за атака на RSA базирани криптографски системи.

Рецензентът приема напълно приносите, така както са формулирани от кандидата в заключението и постигнати резултати.

IV. ОЦЕНКА НА НАУЧНИТЕ РЕЗУЛТАТИ И ПРИНОСИТЕ

Публикуваните резултати най-общо могат да бъдат разделени на научни, научно-приложни и приложни.

Научни приноси

Научните приноси на кандидата могат да бъдат рецензирани и оценени в следните направления:

- Обогатяване на съществуващите знания;
- Разкриване и доказване на съществени нови страни на съществуваща научна област;

- Приложение на научни постижения в практиката и реализиран икономически ефект.

Научно-приложни приноси

Научно-приложните приноси са в областта на информационната сигурност, криптографските алгоритми, механизми, услуги и приложения.

Приложни постижения

Приложните приноси са в областта на проектиране, разработване и внедряване на математическите модели и алгоритми в конкретни приложения.

Значимостта на приносите може да се оцени по приложимостта им в различните реализирани проекти. Заслужава да се отбележат и внедрените в практиката научноизследователски разработки (проекти, задачи, комплекси и системи).

V. ОЦЕНКА НА АВТОРЕФЕРАТА, ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИЯТА И АВТОРСТВО

Автореферат

Авторефератът към дисертационния труд е оформен съгласно изискванията на закона и правилника. В съдържателната си част той вярно и точно отразява дисертационния труд, а именно: заглавието, целта, задачите, приносите, авторските претенции, получените фактически данни, изводите, препоръките, данните за внедряване и използване на резултатите, справката за приносите и списъка на публикациите по него.

Публикации

По темата на дисертационния труд са представени три публикации:

- [1] Stoianov, Nikolai, and Andrey Ivanov. "Public Key Generation Principles Impact Cybersecurity." Information & Security: An

International Journal 47, no. 2 (2020): 249-260, https://doi.org/10.11610/isij.4717

- [2] Иванов А., Стоянов Н., Анализ на подходите за оценка на устойчивостта на криптографски алгоритми с публичен ключ, Десета международна научна конференция „Научните изследвания и инвестициите в технологични иновации – решаващ фактор за отбраната и сигурността“, ХЕМУС 2020, Пловдив
- [3] Ivanov A.G., Stoianov N.T. (2020) New Approach of Solving Congruence Equation System. In: Dziech A., Mees W., Czyzewski A. (eds) Multimedia Communications, Services and Security. MCSS 2020. Communications in Computer and Information Science, vol 1284. Springer, Cham, https://doi.org/10.1007/978-3-030-59000-0_2

Тези публикации позволяват да се получи цялостна представа за получените резултати и осигуряват необходимата публичност на научните приноси и авторските претенции. Рецензентът счита, че в публикациите са отразени основните резултати на дисертационния труд.

Авторство

Личният принос на кандидата в получаването на резултатите в представените за рецензиране трудове е неоспоримо. Авторството му е без съмнение. Внимателният анализ на съвкупната научна продукция на кандидата позволява да се направи извода, че изброените по-горе научни приноси са изцяло негово лично дело. Не установих плагиатстване и приемам, че трудовете и приносите в него са лично дело на кандидата.

VI. ЛИТЕРАТУРНА ОСВЕДОМЕНОСТ И КОМПЕТЕНТНОСТ НА ДОКТОРАНТА

Списъкът на използваните и цитирани в текста информационни източници (114 заглавия, от които 2 на български език, 77 на английски и

35 Интернет адреса) показват литературната осведоменост и компетентност на докторанта, потвърдени от представените научни и приложни резултати.

VII. КРИТИЧНИ БЕЛЕЖКИ И ПРЕПОРЪКИ

Рецензентът не намира съществени научни грешки в представените разработки и публикации. Критичните бележки към инж. Андрей Иванов направени на предварителната защита са напълно отстранени и рецензентът си позволява да ***отбележи прецизното оформяне на дисертационния труд и автореферата.***

VIII. ЛИЧНИ ВПЕЧАТЛЕНИЯ И АПРОБИРАНЕ НА РЕЗУЛТАТИТЕ

Познавам Андрей Иванов от 2004 година. Работили сме съвместно по няколко проекта, свързани с разработката на криптографски системи за защита на информацията. Запознат съм и наблюдавам неговото научно и кариерно развитие почти непрекъснато. Има широка обща култура, задълбочени и трайни научни интереси в областта на програмирането, изследването и разработването на криптографски системи. Част от представените резултати са реализирани в международни проекти, свързани с изследване и разработване на решения в предметната област. Друга част са реализирани в системи (криптиращи устройства), получили одобрение за използване за защита на информацията в компютърни системи и мрежи. Научните резултати са публикувани в престижни научни издания.

IX. ЗАКЛЮЧЕНИЕ И ОЦЕНКА НА ДИСЕРТАЦИОННИЯ ТРУД

Изразявам абсолютното си убеждение, че инж. Андрей Иванов е

един ерудиран, образован и коректен научен работник и изследовател. Общата му оценка, както и конкретната оценка на научните и практически резултати и приноси ми дават основание за изразя своето ***положително становище и твърдата ми увереност***, че представените за рецензиране дисертационен труд, автореферат и публикации по темата на изследването отговарят на изискванията за придобиване на образователната и научна степен „доктор" и да предложа на членовете на уважаемото жури да гласуват ***ПОЛОЖИТЕЛНО*** за даване на ***образователната и научна степен „доктор",*** област на висшето образование ***5. Технически науки***, професионално направление ***5.2 Електротехника, електроника и автоматика***, научна специалност ***Автоматизирани системи за обработка на информация и управление*** на кандидата Андрей Иванов.

13.02.2023 г.
гр. София

Член на журито:
/проф. д.т.н. Веселин Целков/