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.н. инж. Жанета Николова Савова
катедра „Компютърни системи и технологии“, факултет „Артилерия, ПВО и КИС“ на Национален военен университет „Васил Левски“
члена на научното жури

на дисертационния труд на инж. Андрей Георгиев Иванов
автора на дисертационния труд

на тема **„Анализ на устойчивостта на криптографски системи с публичен ключ”**

за придобиване на образователната и научна степен **„доктор”**

докторска програма
„Автоматизирани системи за обработка на информация и управление“
област на висшето образование **5. „Технически науки“**
професионално направление **5.2 „Електротехника, електроника и автоматика“**

1. Актуалност и значимост на разработвания научен проблем

Актуалността на проблема за изследване на устойчивостта на най-използваната в момента асиметрична RSA криптосистема е неоспорима, поради факта, че над 90% от защитата на съвременните интернет комуникации използват този метод. Фактът, че през 2017 г. е открита критична уязвимост CVE-2017-7526 в GPG (Gnu Privacy Guard) библиотеката, която позволява да се разбие RSA-1024 и да се получи ключа, с който да се декриптира съобщението, потвърждава актуалността на изследвания в дисертационния труд проблем. Значимостта на проблема е още повече неоспорима днес, в началото на ерата на реалните квантови изчисления и комуникации, когато група китайски изследователи са предложили практически алгоритъм и са изчислили, че е възможно да го мащабират за атака на 2048-битови RSA ключове, използвайки квантов компютър само с 372 кюбита. Такъв квантов компютър реално съществува, това е IBM Osprey, който е 443 кюбитов процесор.

2. Оценка на научните резултати и приносите на дисертационния труд

Основните приноси на дисертационния труд класифицирам като научно-приложни и приложни:

1. Предложен е модел за оценка на делимостта на дадено цяло число, базиран на алгоритъма на Милър-Рабин, който позволява постигане на детерминистичен резултат без да намалява бързодействието спрямо това на алгоритъма на Милър-Рабин.
2. Предложен е модел на решаване на системи конгруентни уравнения, при който не съществуват ограничаващи условия за числата, с които се изчислява модулната аритметика, да са взаимно прости. Този модел е приложен съвместно с алгоритъма за атака на RSA, предложен от Похлиг-Хелман, за което авторът твърди, че повишава бързодействието на атаката.

3. Синтезиран и математически обоснован е клептографски алгоритъм за атака на RSA базирани криптографски системи. Направен е сравнителен анализ и оценка на устойчивостта на системата в зависимост от избора на генерираната двойка RSA ключове.

Считам, че приносите имат полезност и практическа приложимост в криптоанализа на RSA базирани криптосистеми, като те могат да се определят като обогатяване и доразвиване на вече съществуващи научни проблеми, модели и алгоритми, получаване на потвърдителни факти и прилагането им в практиката.

Убедена съм, че резултатите от извършените в дисертационния труд изследвания и на публикациите по него са лично дело на инж. Андрей Георгиев Иванов и потвърждават значимостта на постигнатите приноси за практическото приложение на RSA криптоанализа.

3. Критични бележки

Извършена е огромна по обем изследователска работа с висока практическа приложимост, но, по мнение на рецензента, могат да се отбележат някои пропуски, бележки и препоръки:

1. Не са достатъчно добре описани и статистически изследвани резултатите от предложените модели и алгоритми. Използвани са изрази като „бяха изпълнени редица тестове“ (стр. 91), „бе направен анализ, включващ редица тестове“ (стр. 93). Препоръчвам на автора да продължи своите статистически изследвания на предложените модели и алгоритми.
2. Препоръчвам на автора да се запознае с алгоритъма на немския математик Schnorr, който през 2021 г. предлага бърз алгоритъм за факторизация чрез използване на SVP (Shortest Vector Problem) алгоритми, както и с публикациите на китайските учени, предлагащи комбинирано прилагане на алгоритъма на Schnorr с

алгоритъма за квантова приблизителна оптимизация QAOA (Quantum Approximate Optimization Algorithm) за разбиване на RSA-2048.

4. Заключение

Считам, че дисертационният труд на тема **„Анализ на устойчивостта на криптографски системи с публичен ключ“**, разработен от инж. Андрей Георгиев Иванов, има качества на напълно завършен в научно-приложно отношение труд по актуални проблеми, свързани с устойчивостта на съвременните асиметрични криптографски системи. Той съдържа значими за практиката научно-приложни резултати, които са лично дело на автора и потвърждават способността му самостоятелно да формулира и разработва важни за практиката проблеми в професионалното направление „Електротехника, електроника и автоматика“ и научната специалност “Автоматизирани системи за обработка на информация и управление”.

Представените дисертационен труд и автореферат отговарят напълно на изискванията на Закона за развитието на академичния състав в Република България и Правилника за неговото прилагане за придобиване на научна и образователна степен **„доктор“**.

5. Оценка на дисертационния труд

Въз основа на гореизложеното давам **положителна оценка** на представените дисертационен труд и автореферат към него. Предлагам на уважаемите членове на научното жури да присъдят на инж. Андрей Георгиев Иванов образователна и научна степен **„доктор“** по научна специалност **„Автоматизирани системи за обработка на информация и управление“**, област на висшето образование **5 „Технически науки“**, професионално направление **5.2 „Електротехника, електроника и автоматика“**.

11.02.2023 г.

Член на журито:

проф. д.н. инж. Жанета Савова