Голові спеціалізованої вченої
ради Д 26.185.01

ВІДГУК
офіційного опонента Зінченка Ярослава Вікторовича
щодо дисертації Міська Віталія Миколайовича за темою «Обчислювальні методи на основі квадратичного решета при криптоаналізі RSA алгоритму апаратно-програмними засобами», поданої на здобуття наукового ступеня кандидата технічних наук за спеціальністю 01.05.02 – математичне моделювання та обчислювальні методи

Актуальність теми дисертації. Широке впровадження у сфери життєдіяльності держави локальних і глобальних інформаційних систем, зокрема, в ті сфери діяльності, що пов'язані з управлінням державою, створює реальні передумови для несанкціонованого використання інформації, яка є власністю держави чи особи, несанкціонованого доступу до інформаційних ресурсів держави і систем управління ними, розповсюдження повідомлень протиправного змісту, порушення цілісності та доступності інформації тощо.

Одним з найважливіших механізмів забезпечення захисту вказаної інформації являється криптографічний захист інформації. Серед методів криптографічного захисту виділяють асиметричний криптоалгоритм RSA, який де-факто вважається стандартом для багатьох криптографічних сервісів і додатків. Однак відомі приклади компрометації криптоалгоритму RSA, пов'язані з певними його реалізаціями, але в загальному випадку вони не є ефективнішими за задачу факторизації. Тому при дослідженні криптостійкості алгоритму RSA основна увага приділяється вирішенню задачі факторизації її криптомодуля, для чого застосовуються кращі серед алгоритмів факторизації та використовуються останні технічні досягнення.

На даний час найефективнішим методом факторизації є метод решета числового поля, а для чисел розміром до 110 десяткових знаків – метод квадратичного решета (QS – quadratic sieve). Відносна простота останнього сприяла виникненню багатьох його модифікацій. При цьому відмічається, що основною проблемою є складність пошуку B-гладких чисел. Число B-гладких є відносно більшим при $X = X_0 = \left\lfloor \sqrt{N} + 1 \right\rfloor$ та швидко зменшується при відхиленнях X від X_0. Тому кращою модифікацією QS вважається метод множинного квадратичного решета (MPQS – multiple polynomial quadratic sieve), в якому B-гладкі шукають серед остач $y_{a,b}(X) = (aX + b)^2 - N$, де a, b – спеціально підібрані цілі числа. В порівнянні з методом QS при $a > 1$ для поліномів $y_{a,b}(X)$ в a раз зменшується кількість можливих значень пробних X при тому ж радіусі просіювання. В той же час не досліджувалося використання поліномів виду $y_k(X) = X^2 - kN$, для яких при більшості значень k кількість пробних X в інтервалі просіювання залишається такою ж, як і для методу QS.

Тому дисертаційна робота Міська В.М., яка присвячена зменшенню обчислювальної складності методів факторизації при вирішенні завдань криптоаналізу алгоритму RSA – удосконаленню існуючих та розробці нових обчислювальних методів факторизації на основі методів QS та MPQS, є актуальною і має практичне значення.

Нові наукові результати дисертації, їх новизна, обґрунтованість, достовірність, теоретична та практична цінність. Аналіз результатів дисертаційної роботи здобувача показує, що *найбільш суттєвими новими науковими результатами*, які одержані ним у дисертації, є:

1. Метод множинного квадратичного k-решета (MQkS), в якому застосовується новий поліном $y_k(X) = X^2 - kN$, (k – натуральне число).

2. Метод діагоналізації матриці «на ходу» та метод визначення достатньої кількості B-гладких чисел.

3. Модифікації методів MQkS, QS, та MPQS – умовно B-гладкі (де B-гладкими називають такі остачі $y_k(X)$, що $y_k(X) = y1(X) \cdot y2(X)$, де $y1(X)$ є добутком простих чисел з факторної бази, а $y2(X)$ – квадратом цілого числа).

4. Способи реалізації методу MQkS на апаратно-програмних засобах, які включають кластери та графічні процесори, в якому враховуються обмеження на стандартні типи даних та обсяг доступної пам'яті, а виконання арифметичних операцій з багаторозрядними числами замінюються операціями з числами типу long (чи long long) та double.

Новизна отриманих наукових результатів здобувача полягає в наступному:

1. Вперше розроблено метод множинного квадратичного k-решета (MQkS), в якому застосовується новий поліном $y_k(X) = X^2 - kN$ (k – натуральне число), що призвело до зменшення в 6 та більше разів кількості пробних X, на основі яких шукають B-гладкі у порівнянні з методом QS, та зменшується час пошуку B-гладких вдвічі для діапазону чисел що розглядалися в роботі.

2. Запропоновано метод діагоналізації матриці «на ходу» та метод визначення достатньої кількості B-гладких чисел, що в окремих випадках може забезпечити розкладання криптомодуля N на множники раніше ніж будуть знайдені B-гладкі остачі у кількості більших ніж розмір факторної бази (незалежно від величини числа N). Даний результат може бути використаний для методів MQkS, QS, та MPQS.

3. Розроблено модифікації методів MQkS, QS, та MPQS – умовно B-гладкі (де B-гладкими називають такі остачі $y_k(X)$, що $y_k(X) = y1(X) \cdot y2(X)$, де $y1(X)$ є добутком простих чисел з факторної бази, а $y2(X)$ – квадратом цілого числа). Показано, що існують випадки, коли на основі застосування запропонованої модифікації можливе скорочення часу отримання достатньої кількості B-гладких, хоча спосіб виявлення умовно B-гладких є дуже затратним в обчислювальному плані та необхідні подальші дослідження стосовно способів їх отримання.

4. Запропоновано способи реалізації методу MQkS на апаратно-програмних засобах, які включають кластери та графічні процесори, в якому враховуються обмеження на стандартні типи даних та обсяг доступної пам'яті, а виконання арифметичних операцій з багаторозрядними числами, замінюються операціями з числами типу long (чи long long) та double.

Обґрунтованість і достовірність нових наукових положень, висновків і рекомендацій.

Наукові положення, висновки і рекомендації, які сформульовані в дисертаційній роботі Міська В.М., в цілому достатньо обґрунтовані. Для теоретичного обґрунтування наукових досліджень та висновків дисертаційної роботи автором коректно застосовано: методи теорії чисел, теорії оптимізації при аналізі методів факторизації чисел та їх модифікацій, методи теорії складності обчислень при дослідженні степені прискорення запропонованих модифікацій, чисельні методи, теорії алгоритмів та комп'ютерного моделювання при перевірці адекватності запропонованого чисельного методу. До реалізації чисельних методів застосовується системний підхід, а саме блочно-ієрархічний та об'єктно-орієнтований підходи. На етапі дослідження запропонованих та реалізованих чисельних методів використовуються чисельний експеримент та методи його обробки.

Основні результати дослідження були отримані для діапазону чисел розмірів 68-107 біт. Висновки, які були зроблені на основі отриманої статистики для діапазону чисел, що розглядався, імовірно можна розширити для всіх чисел, які застосовуються при використанні алгоритму RSA.

Достовірність викладених результатів забезпечується строгістю постановки задачі з урахуванням відповідних обмежень та використанням сучасних чисельних методів їх рішення, а також системним підходом до розробки та тестування програмного комплексу, який експериментально підтверджує теоретичні оцінки, апробацією основних результатів на представницьких наукових конференціях.

Теоретична цінність результатів дисертації полягає в тому, що автор отримав результати, які сприяють подальшому розвитку теоретичних і методологічних основ методів обчислювальної математики стосовно до задач асиметричної криптографії, що використовуються в національних інформаційно-телекомунікаційних системах.

Практична цінність результатів дисертації полягає в тому, що розроблений обчислювальний метод MQkS та його модифікації дозволяють підвищувати швидкодію апаратно-програмних засобів, які використовуються при проведенні тематичних досліджень асиметричних криптоалоритмів, за рахунок використання поліномів $X^2 - kN$ та методів діагоналізації матриці на ходу або визначення достатньої кількості B-гладких, а також врахування обмежень апаратно-програмних засобів за рахунок вибору значень параметрів методу MQkS.

Результати дисертаційної роботи реалізовані в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, а також використані в навчальному процесі ІСЗЗІ КПІ ім. Ігоря Сікорського (в курсі лекцій та практичних занять з навчальних дисциплін «Теоретична криптологія», «Математичні методи побудови та аналізу асиметричних криптосистем»).

Повнота викладу основних результатів дисертації в опублікованих працях. Аналіз дисертаційної роботи та праць здобувача показали, що основні наукові положення опубліковані в період з 2015 по 2019 рік. Основний зміст дисертаційної роботи достатньо повно відображено у 18 наукових публікаціях. Із них 9 статей у науково-фахових виданнях і збірниках у галузі технічних наук

України (з них: 1 стаття іноземною мовою, яка включена до міжнародної наукометричної бази Scopus); 9 тез доповідей – на міжнародних та всеукраїнських конференціях.

Конкретний особистий внесок здобувача в науковій роботі, які написані у співавторстві, відображені як в дисертації, так і в авторефераті.

Мова та стиль дисертації та автореферату. Дисертація написана достатньо грамотно, а стиль викладення в ній матеріалів досліджень, наукових положень, висновків та рекомендацій в цілому забезпечує доступність та легкість їх сприйняття.

Автореферат ідентичний за змістом з основними положеннями дисертації і достатньо повно відображає актуальність, мету та задачі, основні наукові положення, практичну значущість, апробацію дисертації, її зміст по розділах та висновки. Дисертаційна робота та автореферат оформлені у відповідності з вимогами, що ставляться до кандидатських дисертацій в Україні.

Зауваження та недоліки до тексту дисертації та автореферату:

1. В дисертації представлений детальний опис використання графічних карт але відсутні результати тестування представленого чисельного методу на рекомендованому апаратному рішенні. В той же час слід відмітити, що побудова апаратно-програмного комплексу, який представлений у роботі, потребує значних фінансових витрат і даний час не є досяжним.
2. В другому розділі дисертації представлено дослідження розподілу B-гладких, в той же час у першому розділі описується вже існуюча в літературі інформація про розподіл B-гладких.
3. При описі структури апаратно-програмного комплексу не в усіх його модулях вказано, які програмні пакети в ньому застосовано та чітко не сформульовано протоколи взаємодії між ними.
4. В авторефераті дисертації вказано, що розмір необхідної пам'яті для роботи етапу просіювання у методі MQkS становить 62 kB, що є опискою. В дисертації вказано, що розмір колективної пам'яті становить 48 kB, а розмір необхідної пам'яті для роботи просіювання у методі MQkS становить 42 kB.

Однак зазначені вище недоліки не впливають на основні наукові результати і не зменшують високого наукового і практичного рівня дисертації здобувача.

Загальні висновки до дисертаційної роботи.

Дисертаційна робота Міська Віталія Миколайовича на тему «Обчислювальні методи на основі квадратичного решета при криптоаналізі RSA алгоритму апаратно-програмними засобами» є завершеною науковою працею, в якій отримані нові, науково обґрунтовані та практичні результати, що вирішують важливу та актуальну науково-технічну задачу розробки і модифікації обчислювальних методів на основі квадратичного решета при криптоаналізі алгоритму RSA.

Мета роботи, поставлені та розв'язані в ній завдання, викладені основні наукові результати дозволяють зробити висновок про те, що дисертаційна робота відповідає паспорту наукової спеціальності 01.05.02 – математичне моделювання та обчислювальні методи та відповідає профілю спеціалізованої вченої ради Д 26.185.01.

ВИСНОВОК: Дисертаційна робота Міська В.М. за своїм змістом відповідає вимогам п.п. 9, 11 «Порядку присудження наукових ступенів», затвердженого постановою Кабінету Міністрів України № 567 від 24.07.2013 (зі змінами, затвердженими постановами Кабінету Міністрів України № 656 від 19.08.2015, № 1159 від 30.12.2015, № 567 від 27.07.2016) стосовно кандидатських дисертацій, а її автор заслуговує на присудження йому наукового ступеня кандидата технічних наук за спеціальністю 01.05.02 – математичне моделювання та обчислювальні методи.

Офіційний опонент

начальник науково-дослідної спеціальної лабораторії
№ 1 науково-дослідного центру Інституту спеціального
зв'язку та захисту інформації Національного технічного
університету України "Київський політехнічний інститут
імені Ігоря Сікорського"
к.т.н., с.н.с Ярослав ЗІНЧЕНКО
19. 09. 2019

Підпис Зінченка Я.В. засвідчую
Начальник сектору комплектування, проходження
служби та архіву відділу кадрової роботи
ІСЗЗІ КПІ ім. Ігоря Сікорського
Іван ІГНАТЕНКО
19.09.2019