ВІДГУК

офіційного опонента на дисертаційну роботу МІСЬКА Віталія Миколайовича " Обчислювальні методи на основі квадратичного решета при криптоаналізі RSA алгоритму апаратно-програмними засобами " подану на здобуття наукового ступеня кандидата технічних наук за спеціальністю 01.05.02 – математичне моделювання та обчислювальні методи

Дисертаційна робота Міська В.М. присвячена розробці математичних методів факторизації великих чисел на основі ідей методу квадратичного решета та способів їх реалізації з використанням сучасних апаратних засобів при врахуванні обмежень на розмір пам'яті та стандартні типи даних, що важливо при тематичних дослідженнях RSA-алгоритму.

Актуальність постановки задачі. Забезпечення захисту інформації на даний час є одним з найбільш пріоритетних завдань в світі, для чого застосовуються, в тому числі, засоби криптографічного захисту інформації (КЗІ), які допущено до експлуатації. Серед методів криптографічного захисту виділяють асиметричний криптографічний алгоритм (АКА) RSA, який на даний час є стандартом для багатьох криптографічних сервісів і додатків.

Для КЗІ використовуються криптосистеми і засоби криптографічного захисту, які допущені до експлуатації. Допуск до експлуатації – це комплекс організаційно-технічних заходів щодо проведення тематичних досліджень засобів КЗІ, криптографічних досліджень алгоритмів, що використовуються в таких засобах. А обов'язковим етапом проведення криптографічних досліджень є оцінка стійкості криптографічних алгоритмів та протоколів, що використовуються. Оцінка криптостійкості ґрунтується на алгоритмічній складності проведення криптоаналізу таких алгоритмів і повинна враховувати сучасні обчислювальні методи та останні технічні досягнення, що можуть бути використані для оцінки криптографічних якостей алгоритму.

Результати досліджень щодо методів криптоаналізу алгоритму RSA широко представлені в літературних джерелах і встановлено, що відомі приклади компрометації RSA алгоритму пов'язані з певними його реалізаціями, а в загальному випадку не ефективніші за задачу факторизації. Тому при дослідженні стійкості системи шифрування RSA значна увага приділяється вирішенню задачі факторизації її критптомодуля. І у випадку, коли RSA криптомодуль не вдається розкласти на множники (на два багаторозрядних простих числа), даний етап перевірки криптостійкості вважається успішно пройденим. Проте немає актуальної інформації про останні досягнення у методах факторизації криптомодуля RSA алгоритму, якою може володіти зловмисник. Остання обставина визначає необхідність подальших досліджень стосовно розробки методів факторизації та можливостей використання сучасних апаратних засобів.

Серед багатьох методів факторизації метод квадратичного решета (QS – quadratic sieve) займає друге місце у списку найшвидших алгоритмів. Його відносна простота сприяла виникненню багатьох модифікацій, де краща серед них – метод множинного квадратичного решета (MPQS) в якому B-гладкі числа шукають серед остач $y_{a,b}(X) = (aX + b)^2 - N$, де a, b – спеціально підібрані цілі числа.

Для методів QS та MPQS основні проблеми це - складність пошуку B-гладких чисел та значний розмір матриці системи рівнянь. На час факторизації суттєво впливає розвиток технічних засобів. Проте методи QS та MPQS вимагають значного обсягу пам'яті для своєї реалізації що унеможливлює використання сучасних апаратних засобів (включаючи графічні карти). В зв'язку із чим виникає протиріччя між технічними можливостями сучасних апаратних засобів та існуючими способами алгоритмічної реалізації таких методів факторизації. Тому необхідною є адаптація методу факторизації до можливостей апаратних реалізацій стосовно способів обробки даних при обмеженнях на обсяг доступної пам'яті та використання стандартних типів даних.

У зв'язку з цим актуальною є **наукова** задача удосконалення існуючих або розробка нових сучасних обчислювальних методів факторизації на основі методів QS та MPQS, які можна використовувати в сучасних апаратно-програмних комплексах, що забезпечить зниження обчислювальної складності в порівнянні з уже існуючими методами QS та MPQS при вирішенні завдань криптоаналізу RSA алгоритму.

Актуальність теми дисертаційної роботи Міська В.М. підтверджується також тим, що дисертаційні дослідження проводились в рамках НДР «Розвиток методів зниження енергоспоживання обчислювальних систем за рахунок оптимізації обробки масивів даних (шифр – ФРІСК)», (д/р № 0114U000879), НДР «Дослідження та розробка методів оцінювання захищеності інформації в розподілених високопродуктивних інформаційних системах при вирішенні задач енергетики (Шифр МОД-Д)», (д/р 0114U002361), що виконувалась в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

Структура та зміст роботи.

Огляд робіт за тематикою дисертаційної роботи зроблено **в розділі 1**, а основні теоретичні положення роботи викладені в розділах 2 – 4.

В розділі 1 дано аналіз сучасних обчислювальних задач інформаційної безпеки. Представлено алгоритми зашифрування та розшифрування на основі RSA-алгоритму та найбільш широко вживані обчислювальні методи факторизації при криптоаналізі RSA-алгоритму. Описано основні кроки алгоритму квадратичного решета, оцінку обчислювальної складності алгоритму та наведено приклад використання методу QS при факторизації варіанту числа N. Наведено інформацію стосовно ряду модифікацій методу QS

та особливостей практичної реалізації методів QS та MPQS включаючи: можливість роботи з великими числами, наявність різноманітної швидкої пам'яті (в тому числі значний розмір пам'яті для вирішення матриці), швидкі модулі виконання арифметичних операцій, паралелізація та розподілені обчислення. Визначено вимоги до апаратних засобів при реалізації пропонованих алгоритмів, де повинні враховуватися переваги GPU такі як легкість створення потоків, та враховувати недоліки – нестачу пам'яті та наявність різних видів цієї пам'яті, що потребує реалізації спеціального представлення великих чисел та роботи з ними.

Визначені завдання досліджень, які включають вирішення завдань стосовно: прискорення процесу просіювання (збільшення числа B-гладких, при сталому розмірі факторної бази), прискорення вирішення матриці та адаптації алгоритму до обраної апаратної реалізації.

У **розділі 2** представлено матеріали стосовно нового, запропонованого автором методу множинного квадратичного k-решета (MQkS).

Розділ 2.1 присвячений дослідженням стосовно розміщення B-гладких чисел в інтервалі просіювання для відносно малих чисел. Отримані результати ґрунтуються на матеріалах чисельних експериментів. Описані умови їх проведення та наведені висновки. Більшість з висновків відповідає відомим результатам. Новим тут є те, що при збільшенні розміру факторної бази (ФБ) функція числа B-гладких в залежності від її розміру росте не повільніше ніж квадратична. Наведені табличні дані також відображають відомі результати, що при зменшенні розміру ФБ збільшується число варіантів N, для яких не буде знайдено достатню кількість B-гладких. Причому при двократному зменшенні її розміру достатньої кількості B-гладких не було знайдено практично для половини чисел N.

Отримані такі результати дозволили зробити припущення, що при пошуку B-гладких на основі використання багатьох поліномів з малою областю просіювання є ймовірність отримати модифікацію алгоритму методу QS (MPQS), обчислювальна складність якого буде нижчою, оскільки B-гладких чисел більше при малих x з інтервалу просіювання. Використання такої ідеї в літературних джерелах не виявлено.

В **розділі 2.2** проводилися дослідження стосовно оцінки середнього значення числа елементів ФБ при фіксованій границі гладкості для поліномів $y_k(X) = X^2 - kN$. Необхідність даного дослідження обґрунтовується автором тим, що при різних k різними будуть елементи ФБ та їх кількість. Тому пропонується розглядати загальну факторну базу (ЗФБ), серед елементів якої будуть визначатися елементи поточної ФБ, що відповідає конкретному значенню k, де ЗФБ є множиною всіх найменших простих чисел починаючи з 2, кількість яких фіксовано. Результати досліджень отримані на основі чисельних експериментів, умови проведення яких описані.

Для ряду множин чисел N розглядалися варіанти границі гладкості, яка визначалася порядковим номером простого числа, який рівний L^a

($L^a = e^{0/25\sqrt{2\ln N \ln\ln N}}$) та $2L^a$. При цьому K - максимальне значення для k вибиралися рівними $2L^a$, $4L^a$ та $(L^a)^2$, але не розглядалися k, що ділиться націло на квадрат простого числа, яке не перевищує $\sqrt{B}$. За результатами розрахунків встановлено, що середнє число елементів ФБ для всіх варіантів розрахунків несуттєво перевищує половину кількості простих чисел з ЗФБ. В подальшому було встановлено, що час пошуку достатнього числа B-гладких пропонованим методом MQkS для різних N відрізняється несуттєво на відміну від методу QS, де різниця в часі є суттєвою.

В розділі 2.3 досліджується можливість зниження обчислювальної складності процесу просіювання пробних значень на основі використання сигнальних остач $y^*_k(X)$ - добутків перших степенів множників $y_k(X)$, що є елементами факторної бази. При попередньому просіюванні пропонується залишати для подальшого аналізу ті з остач $y_k(X)$, для яких $log(y^*_k(X)) \geq h \cdot log(y_k(X))$, де $h \in [0, 1]$. При такому попередньому просіюванні можливі варіанти, коли при наявності в $y_k(X)$ множників з показниками степеня більше одиниці будуть виключені деякі з B-гладких чисел. Оцінка кількості таких чисел проводилася на основі чисельних експериментів для описаної множини чисел N, що є добутком двох великих простих. На основі отриманих результатів зроблено висновок, що з ростом значення параметру h збільшується кількість відсіяних X та суттєво зменшується кількість тих з пробних X, серед яких слід шукати B-гладкі остачі $y_k(X)$. Тому на основі чисельних експериментів визначався час пошуку достатньої кількості B-гладких чисел в залежності від параметра h. Як випливає з даних табл. 2.7, час пошуку достатньої кількості B-гладких зменшився майже вдвічі, що підтвердило ефективність використання запропонованої процедури попереднього просіювання.

Для можливостей подальшого зниження обчислювальної складності процедури пошуку достатньої кількості B-гладких проводилися дослідження стосовно характеру розподілу більших за одиницю показників степеня множників B-гладких. Оскільки при перевірках подільності $y_k(X)$ лише на першу степінь простого для частини його множників зменшиться кількість операцій з визначення B-гладких, це може призвести до зменшення часу визначення достатнього числа B-гладких. При виділенні такої частини множників запропоновано використовувати параметр *kff*, де допустимими B-гладкими вважалися ті, для яких показники степені їх дільників p могли бути більшими за одиницю при порядкових номерах простих чисел $f_p \leq (L^a)^{kff}$.

Згідно результатів чисельних експериментів, наведених в табл.2.8 для чисел, близьких до $N = 10^m$, де найкращий час розрахунку отримано: при *kff*=0.7 для $m = 20 \div 23$; при *kff* = 0.6 для $m = 24 \div 26$ і для $m = 27 \div 32$ при *kff*=0.5. В усіх випадках час розрахунку знизився не менше ніж в 1.5 рази.

В **розділі 2.4** описано алгоритм методу множинного квадратичного k-решета. В рамках загального опису алгоритму використані такі параметри:

границя гладкості B, розмір радіусу просіювання L (значення яких слід буде вибрати), а також h та kff при попередньому просіюванні на основі сигнальних остач . В описаному алгоритмі передбачено визначати необхідну кількість B-гладких чисел, і тільки після цього виконувати їх обробку.

В **розділі 2.5** представлена інформація стосовно реалізації кроків методу MQkS.

Матеріали досліджень стосовно впливу розміру загальної факторної бази на час отримання достатньої кількості B-гладких представлені **в розділі 2.6**. Розмір ЗФБ визначається через параметр *pla* і зменшується при зменшенні *pla*. Згідно отриманих даних чисельних експериментів, представлених в табл.2.9, при зменшенні значення параметра *pla* зростає час розрахунку для всіх аналізованих чисел N, при чому темп зростання збільшується при зменшенні *pla*. Характерним також є зменшення значення параметра *kff* при збільшенні N. Тому для вибору розміру ЗФБ та параметру *kff* доцільно отримати оцінку обчислювальної складності алгоритму пропонованого методу MQkS з просіюванням на основі сигнальних остач.

Розділ 2.7 присвячений оцінці обчислювальної складності алгоритму формування достатньої кількості B-гладких з проріджуванням пробних X на основі сигнальних остач. Визначено загальний вид залежності, на основі якої може бути описано характер асимптотичної оцінки обчислювальної складності виду $T(N) = O(\exp(C\sqrt{\ln N \ln\ln N}))$. Дослідження стосувалися оцінки коефіцієнта C. Отримані результати ґрунтуються на матеріалах чисельних експериментів, в яких визначався час пошуку достатньої кількості B-гладких для описаної множини чисел N порядку 10^m при $m = 20 \div 32$. В чисельних експериментах приймалися фіксованими значення параметрів *plb* = 1.4 та h=0.7, а значення параметрів *pla* та *kff* змінювалися. Показано, що для аналізованої множини чисел N при *pla* = 0.94 та $kff \le 0.6$ коефіцієнт C приймає значення менше за одиницю, де у відомих оцінках для методів QS і MPQS C в кращому випадку є величиною $1 + o(1)$.

Висновки по розділу наведено в **розділі 2.8**.

Розділ 3 присвячений знаходженню коренів СЛАУ, де коефіцієнтами матриці є число одиниця, якщо відповідне B-гладке ділиться на степінь простого числа із ЗФБ, а показник степеня непарний.

В розділі розглядаються питання рішення матриці «на ходу», тобто по ходу визначення B-гладких чисел, способу зниження розміру матриці за рахунок визначення умов, коли кількість B-гладких виявиться достатньою, а також можливості отримання умовно B-гладких, які можуть бути використані в матриці нарівні з B-гладкими числами.

Представлено алгоритм методу вирішення матриці «на ходу». Наведено приклад застосування методу, де розкладання числа N на множники отримано значно раніше, ніж потрібно для визначення кількості B-гладких, що дорівнює числу елементів ЗФБ плюс два. Наведено середні евристичні оцінки стосовно зниження обчислювальної складності алгоритму методу квадратичного решета

для чисел N від 10^{14} до 10^{130}, де для чисел N порядку 10^{130} час розрахунку зменшиться орієнтовно на 5.45%.

В **розділі 3.3** запропоновано метод діагоналізації матриці, на основі якого необхідний обсяг пам'яті зменшується вдвічі. Описано алгоритм методу, представлено його блок-схему та наведено приклад використання методу.

Ідея досліджень, результати яких представлені в **розділі 3.4**, полягає у використанні суттєво меншої кількості B-гладких чисел при збереженні розміру факторної бази, за рахунок чого можливе суттєве зниження часу факторизації тобто й зменшення інтервалу просіювання. Використання меншої кількості B-гладких виконується завдяки початковому розміру факторної бази $L_{\max} > L^a$ та визначенні достатнього такого розміру L^*, який може виявитися меншим за L^a. Описано алгоритм методу вибору достатньої кількості B – гладких чисел та наведено приклад його застосування.

Розділ 3.5. присвячено використанню умовно B-гладких чисел при пошуку необхідної їх кількості.

Отримані результати є підставою для подальшого дослідження на числах 1024 біт та більше.

Розділ 4 присвячений розробці рекомендацій з апаратно-програмної реалізації розроблених методів при проведенні криптоаналізу RSA-алгоритму.

Практична реалізація розроблених методів була здійснена для однопоточної ЕОМ з використанням мови С. Оцінка такого підходу представлена в **розділі 4.1**.

Оцінка можливості використання паралельних і розподілених обчислень, а також спеціалізованих апаратно-програмних та апаратних засобів для вирішення завдання підвищення їх продуктивності при реалізації розроблених методів, включаючи застосування технології GPGPU CUDA для організації паралельних обчислень.

В **розділі 4.2** наведено результати аналізу існуючих варіантів організації паралельних обчислень. Описано варіанти організації паралельних обчислень таких класів: симетричні мультипроцесорні системи, масивно-паралельні системи, кластерні системи, Grid мережа, паралельні векторні системи, системи з неоднорідним доступом до пам'яті, а також «хмарні» технології.

Представлено варіант класифікації архітектур паралельних обчислювальних систем.

Розділ 4.3 присвячений застосуванню технології GPGPU CUDA для організації паралельних обчислень, де описано архітектуру системи CUDA, структуру пам'яті та особливості реалізації арифметичних операцій з багаторозрядними числами. На основі проведеного аналізу в **розділі 4.4** рекомендується використовувати технологію GPGPU в задачах криптоаналізу RSA-алгоритму, в тому числі для реалізації методу MQkS.

Спосіб розпаралелювання для методу MQkS та вибір значень параметрів для забезпечення обмежень стосовно обсягу пам'яті та стандартних типів

даних графічних карт описано в розділі 4.5, де також схема алгоритму А методу MQkS для реалізації із використанням технології GPGPU CUDA.

Наведено висновки до розділу 4.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій.

Наукові положення, висновки дисертаційної роботи в цілому достатньо обґрунтовані. Для обґрунтування наукових положень автором застосовано методи теорії чисел при формуванні факторної бази та поточної факторної бази, алгоритмічної теорії багаторозрядних чисел при формуванні даних про такі числа для їх подання в комп'ютері, теорії складності обчислень при отриманні порівняльних характеристик обчислювальної складності пропонованих та відомих чисельних методів, методи комп'ютерного моделювання при розробці експериментальних програмних додатків та вирішенні з їх допомогою тестових задач.

Наукові положення і висновки дисертаційної роботи підтверджені шляхом зіставлення з даними чисельних експериментів.

Достовірність результатів досліджень.

Достовірність результатів дисертаційного дослідження забезпечена коректністю постановки математичних задач з урахуванням відповідних обмежень, та використанням сучасних математичних методів, підтверджена узгодженням теоретичних результатів з даними чисельних експериментів, а також апробацією основних результатів на представницьких наукових конференціях.

Отримані результати вважаю обґрунтованими, достовірними та новими.

<u>Наукова новизна дисертаційної роботи полягає в наступному</u>

1. Вперше розроблено метод множинного квадратичного *k*-решета (MQkS – multiple quadratic k-sieve), в якому застосовується новий поліном $y_k(X) = X^2 - kN$ (k - натуральне число), який при більшості своїх варіантів забезпечує пошук B-гладких серед всіх пробних значень в єдиному інтервалі просіювання, в якому на відміну від методів QS та MPQS:
   - Використовуються загальна факторна база та поточна база (для кожного з поліномів).
   - Розмір інтервалу просіювання адаптовано під використання нового поліному.
   - Виконується попереднє просіювання пробних X.
   - При просіюванні пробних X, пошук дільників остач $y_k(X)$, показник степеня яких може перевищувати одиницю, здійснюється для обмеженої кількості простих чисел з поточної факторної бази, за рахунок чого можливе врахування обмежень на обсяг пам'яті та доступні стандартні типи даних апаратних засобів.

Встановлено, що існує діапазон значень параметрів для визначеної множини чисел порядку 10^m, де m=20÷32, отримано значення коефіцієнту $C < 1$ в оцінці складності методу MQkS виду $O\left(exp\left(C\sqrt{ln\,N\,lnln\,N}\right)\right)$. У відомих оцінках обчислювальної складності методів методів QS та MPQS коефіцієнт $C \geq 1$. Для аналізованої множини чисел N порядку 10^m, де m=9÷32 встановлено також, що в порівнянні з методом QS кількість пробних X, на основі яких шукають B-гладкі, в 6 та більше разів перевищує їх кількість для аналогічного числа пробних в методі QS та зменшується час пошуку B-гладких.

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. За рахунок встановлення існування серед остач $y_k(X)$ таких, 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, які названо умовно B-гладкими, запропоновано модифікацію методів MQkS, QS, та MPQS – умовно B-гладкі. 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.

Значущість отриманих результатів для науки і практичного використання.

Значущість отриманих результатів для науки полягає у постановці та вирішенні задачі розробки обчислювальних методів факторизації на основі алгоритму методу квадратичного решета, що дозволяють підвищити швидкодію апаратно-програмних засобів, які використовуються при криптоаналізі RSA алгоритму за рахунок створення більш ефективних методів просіювання і зменшення обчислювальної складності операцій з багаторозрядними числами.

Значущість результатів дисертаційного дослідження для практики полягає у тому, що полягає у тому, що розроблені обчислювальні методи дозволяють підвищувати швидкодію апаратно-програмних засобів, що використовуються при проведенні тематичних досліджень АКА, за рахунок використання попереднього просіювання, а також способів заміни

арифметичних операцій з багаторозрядними числами на операції з числами типу *long*, що при відповідному виборі параметрів методу MQkS дозволяє використання сучасних апаратних засобів для факторизації великих чисел, включаючи графічні карти.

Отримані результати складають теоретичну, методологічну та технічну основу удосконалювання існуючих і створення нових ефективних обчислювальних методів криптоаналізу АКА RSA.

Практичне значення отриманих результатів дисертаційної роботи полягає в тому, що результати роботи дозволяють:

- проектувати більш ефективні, з точки зору швидкодії, апаратно-програмні засоби проведення криптоаналізу АКА та, як наслідок, зменшити строки виконання державних експертиз у сфері КЗІ нових КА;
- здійснювати оцінку криптостійкості АКА RSA з використанням апаратно-програмної архітектури паралельних обчислень за допомогою технології GPGPU.

Основні наукові результати отримали практичне викороистання в наступних організаціях:

- Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського",
- Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України.

Повнота викладення результатів в опублікованих матеріалах. Наукові положення, висновки і рекомендації дисертаційного дослідження опубліковані у 18 роботах, з яких 9 наукових статей – у фахових наукових журналах та збірниках наукових праць, що відповідають вимогам ДАК України, у тому числі 9 у наукових журналах, які індексуються міжнародними наукометричними базами; 9 – публікації матеріалів конференцій.

В опублікованих працях в фахових наукових виданнях повністю викладено основні наукові положення дисертаційної роботи та отримані результати, а рівень та кількість публікацій відповідають вимогам до кандидатських дисертацій в Україні.

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

При загальній позитивній характеристиці роботи є ряд зауважень:

Зауваження:

1. В розділі 1 визначені завдання дослідження, але у висновках до розділу не відображено мету та часткові завдання дослідження.
2. В розділі 3.5.3, присвяченому оцінці складності алгоритму факторизації, в якому додатково використовується пошук умовно B-гладких чисел, відмічається, що до моменту пошуку умовно B-гладких «… Всі залишки y(x) вже отримані, їх пошук не потребує додаткової роботи. …», що не є коректним, оскільки залишки y(x) шукають для пробних значень x, що залишилися після просіювання. В той же час справедливе твердження, що «…можливі випадки отримання кореня коли остача $y(x)$ буде повним квадратом, або кілька умовно B-гладких дозволять сформувати достатню кількість остач, на основі яких буде отримано дільники N …»
3. В розділі 1.2. на стор.32 вказано: «…Процедури генерації ключів, шифрування та дешифрування для цього алгоритму представлені на рис. 1.1…», хоча мова йде про алгоритми генерації ключа, зашифрування та розшифрування шифротексту.
4. Мають місце повторення тексту при визначенні актуальності досліджень.
5. Наявні помилки при посиланнях на формули: на стор.64: замість формули (2.2) вказано (2), а в заголовку таблиці 2.5 замість «…обмеження (4) …» слід писати «…обмеження (2.13)…).
6. Ряд сторінок 75, 77, 95, 100, 147 заповнені тільки частково, хоча при перенесенні тексту перед таблицями чи рисунками цього можна було уникнути.
7. Мають місце стилістичні помилки.

Зроблені зауваження не знижують наукову цінність отриманих результатів, більшою мірою відносяться до її оформлення та не впливають на загальну її позитивну оцінку.

Вважаю, що дисертаційна робота МІСЬКА Віталія Миколайовича "Обчислювальні методи на основі квадратичного решета при криптоаналізі RSA алгоритму апаратно-програмними засобами" за актуальністю, обсягом проведених та використаних досліджень, науковою новизною, практичною цінністю є завершеним науковим дослідженням, відповідає спеціальності 01.05.02 – "Математичне моделювання та обчислювальні методи", в якій запропоновано новий метод MQkS факторизації, багаторозрядних чисел, алгоритм якого характеризується нижчою обчислювальною складністю в порівнянні з методами QS і MPQS та забезпечується можливість використання сучасних апаратно-програмних засобів при вирішенні завдань криптоаналізу АКА RSA. Запропоновані ж методи діагоналізації «на ходу» і визначення достатньої кількості B-гладких дозволяють в окремих випадках забезпечити

розкладання криптомодуля N на множники раніше ніж будуть знайдені B-гладкі остачі $y_k(X)$ у кількості кількості, що перевищує розмір загальної факторної бази. Дисертаційна робота задовольняє вимогам до кандидатських дисертацій згідно п.п. 9, 11 "Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника", затвердженого постановою Кабінету Міністрів України №567 від 24 липня 2013 р., а її автор, Місько Віталій Миколайович заслуговує присудження наукового ступеня кандидата технічних наук за обраною спеціальністю.

Ст.н.с. Відділу спеціалізованих
засобів моделювання Інституту
проблем реєстрації інформації
НАН України д.т.н., ст..н.с. Я.О.Каліновський