**НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ**

**ІНСТИТУТ ПРОБЛЕМ МОДЕЛЮВАННЯ В ЕНЕРГЕТИЦІ ІМ. Г.Є. ПУХОВА**

**МІСЬКО Віталій Миколайович**

УДК 511:003.26.09

# ОБЧИСЛЮВАЛЬНІ МЕТОДИ НА ОСНОВІ КВАДРАТИЧНОГО РЕШЕТА ПРИ КРИПТОАНАЛІЗІ RSA АЛГОРИТМУ АПАРАТНО-ПРОГРАМНИМИ ЗАСОБАМИ

01.05.02 – математичне моделювання та обчислювальні методи

**Автореферат**

дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2019

Дисертацією є рукопис.
Робота виконана в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, м. Київ.

**Науковий керівник:** доктор технічних наук,
старший науковий співробітник
**ВИННИЧУК Степан Дмитрович**,
Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, завідувач відділу моделювання енергетичних процесів і систем

**Офіційні опоненти:** доктор технічних наук,
старший науковий співробітник
**КАЛІНОВСЬКИЙ Яків Олександрович**,
Інститут проблем реєстрації інформації НАН України, старший науковий співробітник відділу спеціалізованих засобів моделювання

кандидат технічних наук,
старший науковий співробітник
**ЗІНЧЕНКО Ярослав Вікторович,**
Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", завідувач науково-дослідної спеціальної лабораторії № 1 науково-дослідного центру

Захист відбудеться "30" вересня 2019 року о 14 годині на засіданні спеціалізованої вченої ради Д 26.185.01 Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, м. Київ, вул. Генерала Наумова, 15.

З дисертацією можна ознайомитись у бібліотеці Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України за адресою: 03164, м. Київ, вул. Генерала Наумова, 15.

Автореферат розісланий "29" серпня 2019 року.

Вчений секретар
спеціалізованої вченої ради Д 26.185.01 В.В. Душеба

## ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Актуальність теми.** Сучасне суспільство все більше стає інформаційно-обумовленим. Завдання забезпечення захисту інформації при її обробці в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах на даний час є одним з найбільш пріоритетних в багатьох країнах світу і, в тому числі, в Україні. Обов'язковою умовою обробки інформації з обмеженим доступом в національних інформаційно-телекомунікаційних системах є застосування засобів технічного та/або криптографічного захисту інформації (КЗІ), які допущено до експлуатації. Рішення про допуск приймається за результатами тематичних досліджень, одним з елементів яких є оцінка криптографічної стійкості криптоалгоритмів, що використовуються в об’єктах досліджень.

Серед методів криптографічного захисту виділяють асиметричний криптоалгоритм (АКА) RSA, який де-факто вважається стандартом для багатьох криптографічних сервісів і додатків. Результати досліджень щодо методів його криптоаналізу представлені в роботах авторів Song Y. Yan, Kocker P.C., Shamir A., D. Genkin, B. Weger Д., Sounak G. and Goutam P., Brown D., Авдошин С.М., Горбенко І.Д. та багатьох інших. Аналіз публікацій показує, 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, для чого застосовуються кращі серед алгоритмів факторизації та використовуються останні технічні досягнення.

Проблема полягає в тому що немає актуальної інформації про останні досягнення у методах факторизації криптомодуля RSA алгоритму, якою може володіти зловмисник. Остання обставина визначає необхідність застосування останніх досягнень стосовно методів факторизації та сучасних апаратних засобів.

Серед багатьох методів факторизації метод квадратичного решета (QS – quadratic sieve) займає друге місце у списку найшвидших алгоритмів, поступаючись тільки методу решета числового поля, а для чисел розміром до 110 десяткових знаків і досі є найкращим. Відносна простота алгоритму сприяла виникненню багатьох його модифікацій. При цьому відмічається що основна проблема це - 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 можна очікувати, що при використанні поліномів $y_k(X)$ та однакового інтервалу просіювання при різних $k$ зменшиться час роботи алгоритму з пошуку достатньої кількості B-гладких та будуть виявлені умови, при яких можливою стане факторизація чисел порядку до $2^{1024}$, що важливо при вирішенні завдань криптоаналізу RSA алгоритму.

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 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.

Таким чином, в дисертації вирішується актуальна **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, що має важливу наукову та практичну спрямованість при удосконаленні існуючих і створенні перспективних апаратно-програмних засобів криптоаналізу АКА RSA.

**Зв'язок роботи з науковими програмами, планами, темами.** 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.

**Мета і завдання дослідження**. Метою роботи є зменшення обчислювальної складності методів факторизації багаторозрядних чисел заснованих на ідеях

методу квадратичного решета, що надасть можливість підвищити швидкодію апаратно-програмних засобів при вирішенні завдань криптоаналізу АКА RSA.

Для досягнення поставленої наукової мети в дисертаційній роботі вирішуються такі *задачі дослідження*:

1. Провести аналіз математичних методів і підходів до оцінки захищеності АКА RSA при проведенні тематичних досліджень. Визначити роль і місце алгоритму факторизації квадратичного решета при оцінці криптостійкості RSA криптоалгоритму.

2. Розробити спосіб максимального використання близьких до $X_0 = \lfloor \sqrt{N} + 1 \rfloor$ значень для отримання необхідної кількості B-гладких чисел.

3. Здійснити аналіз та оцінити можливість ефективного аналізу множини B-гладких чисел для прискорення отримання нульового вектору при рішенні системи лінійних алгебраїчних рівнянь (СЛАР), без збільшення необхідного об'єму пам'яті.

4. Розробити рекомендації стосовно можливості використання запропонованих методів та алгоритмів для апаратних та апаратно-програмних засобів при оцінці криптографічної стійкості RSA-алгоритму.

***Об'єктом дослідження*** **є** процес факторизації багаторозрядних чисел при проведенні криптоаналізу RSA-алгоритму.

***Предметом дослідження*** **є** обчислювальні методи факторизації багаторозрядних чисел, засновані на алгоритмі квадратичного решета, що дозволяють зменшити обчислювальну складність операцій з великими числами, включаючи їх адаптацію до можливостей апаратних реалізацій при використанні в апаратно-програмних комплексах.

**Методи дослідження**. Для вирішення наукової задачі використані методи теорії чисел, теорії оптимізації – для аналізу методів факторизації чисел та їх модифікацій, теорії складності обчислень – для дослідження степені прискорення запропонованих модифікацій, чисельні методи, теорії алгоритмів та комп'ютерного моделювання – перевірка 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.

**Наукова новизна отриманих результатів** визначається наступними положеннями:

1. Вперше розроблено метод множинного квадратичного *k*-решета (MQkS), 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 $O\left(\exp(C\sqrt{\ln N \ln\ln N})\right)$. 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.

**Практичне значення отриманих результатів** полягає у тому що розроблений обчислювальний метод MQkS та його модифікації дозволяють

підвищувати швидкодію апаратно-програмних засобів, що використовуються при проведенні тематичних досліджень АКА, 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.

Зокрема, результати роботи дозволяють:

– додати ще один етап криптоаналізу АКА RSA апаратно-програмними засобами, як наслідок, збільшити ефективність криптоаналізу комерційних та державних експертиз у сфері КЗІ нових криптоалгортимів;

– 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 криптоалгортимів;

– здійснювати оцінку криптостійкості АКА RSA з використанням апаратно-програмної архітектури паралельних обчислень за допомогою технології GPGPU (General-purpose Computing for Graphics Processing Units).

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

Результати роботи реалізовані в Інституті проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, а також використані в навчальному процесі Інститут спеціального зв’язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського”.

**Особистий внесок здобувача.** Всі результати дисертаційної роботи, що винесені на захист, отримані автором самостійно. У роботах, які опубліковано у співавторстві, особисто дисертантові належать наступні результати: [1] – розроблений програмний додаток, проведено розрахунки та здійснено їх аналіз; [2, 10, 11] – алгоритм застосування декількох баз, експериментальне порівняння декількох баз з однією; [3, 12] – обґрунтовано метод достатньої кількості B-гладких, проведено аналіз результатів тестування; [4, 6, 13] – алгоритм умовно B-гладких, експериментальне порівняння зі стандартним методом QS; [5, 14, 15] – алгоритм рішення матриці на ходу, експериментальне порівняння зі стандартним методом QS, та вирішені ряд задач з оцінки складності алгоритму; [7, 16] – розроблено алгоритм методу MQkS, проведено аналіз оцінки впливу розміру факторної бази та інтервалу просіювання на час факторизації; [8, 9, 17, 18] – обґрунтовано метод використання сигнальних остач, та розроблена методика його застосування;

**Апробація результатів дисертації.** Основні ідеї та конкретні наукові результати досліджень доповідались й обговорювались на:

1. “Ускорение метода Ферма факторизации чисел вида n = pq, где p и q простые, методом прореживания.” / В.М. Мисько. // Матеріали XXXIV Науково-технічної конференції «Моделювання» ІПМЕ ім. Г.Є. Пухова НАН України. 13-14 січня 2015 року. – тези доп. – м. Київ. – С.7.
2. “Ускорение метода Ферма факторизации чисел вида n = pq, где p и q простые, методом прореживания с использованием нескольких баз. ” / С.Д. Винничук, В.М. Місько. // Матеріали XXXVI Науково-технічної конференції «Моделювання» ІПМЕ ім. Г.Є. Пухова НАН України. 12-13 січня 2016 року. – тези доп. – м. Київ. – С.22.
3. “Прискорення методу квадратичного решета на основі використання розширеної факторної бази та формування достатньої кількості B-гладких чисел” / В.М. Місько. //ІІІ Міжнародна науково-практична конференція "Інформаційна безпека та комп’ютерні технології" 19-20 квітня 2018 року.: тези доп. – м. Кропивницький., – С. 106-108.
4. “Прискорення методу квадратичного решета на основі пошуку додаткових B-гладких чисел.” / В.М. Місько // Матеріали VI заочної наукової конференції «Наукові підсумки 2017 р», 13.11.2017. Науковий журнал «ScienceRise». – 2017. – №12(41). м. Харків. – С. 67-71. DOI: 10.15587/2313-8416.2017.118298
5. «Прискорення методу квадратичного решета на основі рішення матриці на ходу.» / В.М. Місько // Програма І Міжнародної науково-практична конференції “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS). 05-06 квітня 2018 р,: тези доп. – К., – С. 272-274.
6. «Прискорення методу квадратичного решета на основі рішення матриці на ходу». / В.М. Місько // Щорічна науково-технічна конференція молодих вчених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України. 16 травня 2018 року, м. Київ. ,: тези доп. – К., – С. 29-30.
7. Множинне Квадратичне К-решето (MQKS). / С.Д. Винничук. В.М. Місько // Матеріали VI міжнародної наукової конференції «Моделювання-2018». 12-14 вересня 2018 р.: тези доп. – К., – С. 207-210.
8. Множинне квадратичне k-решето факторизації чисел. / С.Д. Винничук В.М. Місько // Матеріали науково-практичної конференції «Сучасні інформаційні технології та кібербезпека», 15-16 листопада 2018р.: тези доп. – К., – С. 194-197.
9. Метод множинного квадратичного k-решета з використанням сигнальних остач при просіювання пробних значень. / В.М. Місько, С.Д. Винничук // XII Міжнародна науково-практична конференція «Комп’ютерні системи та мережеві технології» 28 –30 березня 2019 року.: тези доп. – К., – С. 27-28.

**Публікації.** 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.

**Структура та обсяг дисертації.** Робота складається з анотації, вступу, чотирьох розділів, висновків, двох додатків та списку використаних джерел зі 147 найменувань. Загальний обсяг дисертації складає 245 сторінки. Основний зміст роботи викладено на 165 сторінках. Дисертація містить 12 рисунків та 38 таблиць.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовується актуальність теми дисертації, формулюються наукова задача і мета роботи, основні напрямки її вирішення і часткові задачі дослідження, зв'язок з науковими програмами, планами і темами. Визначено наукову новизну і практичне значення отриманих результатів. Наведено відомості про апробацію результатів дослідження, публікації та реалізації основних результатів, отриманих у дисертації.

**В першому розділі** дано огляд публікацій за темою дисертаційної роботи та визначено завдання досліджень.

Описано RSA алгоритм та принципи його роботи.

Досліджено питання використання RSA-алгоритму у засобах КЗІ в Україні.

Для визначення напрямів досліджень з обраної тематики проведено аналіз сучасного стану досліджень методів факторизації АКА RSA і їх застосування при проведенні криптоаналізу.

Розглянуто ряд методів факторизації серед яких метод квадратичного решета (**QS**) який і досі є найшвидшим для цілих чисел до 110 десяткових знаків. Для чисел більшого розміру застосовується метод решета числового поля (**GNFS**).

Метод QS влаштований значно простіше, ніж GNFS, що сприяло виникненню багатьох його модифікацій при достатньо легкому його розпаралелюванню.

Наведено означення ряду основних понять, що використовуються у роботі, в тому числі поняття: породжуючого полінома, квадратного лишку, границі гладкості, факторної бази, радіусу просіювання, B-гладкого числа, просіювання.

**Визначення 1.** Поліном $P(X)$, значення якого використовуються в алгоритмі факторизації називається *породжуючим* поліномом.

**Визначення 2.** Число $a$ називається *квадратним лишком по модулю p*, якщо існує ціле число $x$ таке, що остача від ділення $x^2$ на $p$ дорівнює $a$ ( $x^2 (\mathrm{mod} p) = a$).

**Визначення 3.** Число B називається *границею гладкості*, якщо найбільше з простих чисел, що розглядаються як можливий дільник породжуючого полінома $P(X)$ при деякому $X$, не перевищує значення B.

**Визначення 4.** Множина простих чисел, які не перевищують границю гладкості B, де для кожного з простих $p$ існує ціле число $X$ таке, що $P(X) = 0$,

називається *факторною базою*. У випадку породжуючих поліномів $y_k(X) = X^2 - kN$, просте число $p$ буде *елементом факторної бази*, якщо $(kN) \pmod p$ є квадратним лишком для $p$. Число елементів факторної бази позначимо через $fa$.

**Визначення 5.** B-*гладким числом* називається значення полінома $P(X)$, яке розкладається на прості множники, кожен з яких є елементом факторної бази.

**Визначення 6.** *Радіус просіюванням* $L$ – це число, що при $X_0 = \lfloor \sqrt{N} + 1 \rfloor$ визначає діапазон значень $X$: $X_0 - L \le X = X_0 + x \le X_0 + L$ , серед яких шукають B-гладкі числа, де $x \in [-L, L]$.

**Визначення 7.** Для полінома $P(X)=P(X_0+x)$ *просіюванням* (для деякого радіусу L) називається процедура, що визначає які із значень $P(X_0+x)$, де $x \in [-L, L]$, є B-гладкими.

Представлено інформацію стосовно оцінки обчислювальної складності методів QS та MPQS.

Описано способи реалізації процедури просіювання.

Наведено відомі дані щодо розподілу B-гладких чисел. Показано, що B-гладі числа набагато частіше зустрічаються при $X$ близьких до $X_0 = \lfloor \sqrt{N} + 1 \rfloor$.

Відмічено, що на час факторизації суттєво впливає розвиток технічних засобів. Проте для їх використання 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.

Визначено та обґрунтовано завдання досліджень.

В **другому розділі** описаний метод множинного квадратичного k-решета (MQkS). В методі у якості поліномів просіювання використовуються поліноми $y_k(X) = X^2 - kN$.

Для методу QS існує два підходи для визначення розміру факторної бази: на основі границі гладкості, або на основі кількості елементів факторної бази.

Для методу QS рекомендована кількість елементів факторної бази - $L^a = \left(e^{\sqrt{\ln N \ln\ln N}}\right)^{\sqrt{2}/4}$ , а розмір інтервалу просіювання $L^b = \left(e^{\sqrt{\ln N \ln\ln N}}\right)^{3\sqrt{2}/4} = \left(L^a\right)^3$ .

Проте у методі MQkS при зміні k змінюється факторна база у зв’язку із чим пропонується використовувати загальну факторну базу (**ЗФБ**), яка утворена всіма найменшими простими числами починаючи з 2.

Число елементів ЗФБ $fa = \left( \exp\left( \frac{\sqrt{2}}{4} \sqrt{\ln N \cdot \ln\ln N} \right) \right)^{pla} = \left(L^a\right)^{pla}$, де $pla \in [0.5, 1.5]$ – параметр.

При кожному зі значень k з елементів ЗФБ формується поточна факторна база.

Розмір інтервалу просіювання $fb = \left( \exp\left( \frac{\sqrt{2}}{4} \sqrt{\ln N \cdot \ln \ln N} \right) \right)^{plb} = \left(L^a\right)^{plb}$, де $plb$ – це параметр, який визначається на основі чисельних експериментів.

Проведені дослідження стосовно кількості елементів поточної факторної бази в залежності від $k$ при фіксованому розмірі ЗФБ показали, що при різних $k$ в середньому воно більше половини елементів ЗФБ.

На основі аналізу варіантів розкладання ряду чисел N на множники було помічено, що в багатьох випадках показники степенів дільників B-гладкого числа дорівнюють одиниці, тому було введено поняття сигнальних остач $y_k^*(X)$, де $y_k^*(X)$ є добутком перших степенів множників $y_k(X)$. і проводилися оцінки стосовно того, наскільки $\log\left(y_k^*(X)\right)$ перевищує $h \cdot \log\left(y_k(X)\right)$, де $h \in [0,1]$ – параметр. В усіх випадках, коли виконувалася умова $\log\left(y_k^*(X)\right) < h \cdot \log\left(y_k(X)\right)$, пробні X виключалися з подальшого аналізу. Вони вважалися відсіяними та такими, що не належать множині MV($h$) - допустимих пробних $X$ ($X \notin MV[h]$), а факт виконання умови $\log\left(y_k^*(X)\right) \geq h \cdot \log\left(y_k(X)\right)$ позначався $X \in MV[h]$.

В результаті проведених чисельних експериментів стосовно використання параметру $h$ було показано, що для чисел розміром $10^{20}$-$10^{32}$ кращий час отримано при для $h$ = 0.7÷0.8. Тоді час розрахунку виявився майже вдвічі меншим, за відповідний час розрахунку при $h$ = 0, коли B-гладкі шукали серед остач $y_k(X)$ для всіх пробних $X$.

З ростом $N$ зростає відносна кількість B-гладких, у яких всі показники степеня множників $y_k(X)$ дорівнюють одиниці, тобто значення $h$ збільшується, де при $h$ = 1 до множини B-гладких ввійдуть тільки остачі $y_k(X)$, які є добутком простих чисел з поточної факторної бази, показник степеня яких дорівнює 1.

Вибравши деяке фіксовані значення параметрів $h$ та $plb$ було проведено більш детальний аналіз дільників B-гладких чисел. Відмічено, що з ростом $N$ зростає відносна кількість множників B-гладких, для яких показники степеня множників дорівнюють одиниці, а більші за одиницю показники степеня характерні для відносно малих значень простих $p$ та рідко зустрічаються при більших $p$. Тому пропонується шукати дільники B-гладких чисел, показники степеня яких перевищують одиницю, для відносно малих значень елементів факторної бази, що не перевищують деякої границі. Для визначення такої границі запропоновано використовувати параметр $kff$.

При використанні параметру $kff$, допустимими B-гладкими вважалися ті, для яких показники степені їх дільників $p$ могли бути більшими за одиницю при виконанні умови

$$f_p \leq ff = (L^a)^{kff}, \qquad (8)$$

де $f_p$ – порядковий номер простого $p$ у списку простих чисел, *kff* – дійсне число, значення якого змінюються в діапазоні від 0 до 1, при значення *kff* = 1 відсутні обмеження для $f_p$, а при *kff* = 0 до B-гладких будуть віднесені тільки ті з остач $y_k(X)$, для яких має місце рівність $y_k(X) = y_k^*(X)$.

Для оцінки ефективності параметру kff проводився ряд чисельних експериментів.

Чисельні експерименти показали:

- для $m = 20 \div 23$ кращий час при *kff* = 0.7, що в 1.2 рази швидше ніж для *kff* =1;
- для $m = 24 \div 26$ кращий час при *kff* = 0.6, що в 1.35 рази швидше ніж для *kff* =1;
- для $m = 27 \div 32$ кращий час при *kff* = 0.5 що в 1.55 рази швидше ніж для *kff* =1.

Тобто з ростом *N* доцільно зменшувати значення параметра *kff*.

Загальний алгоритм **A** методу MQkS описується наступними кроками.

1. Для заданого N задати значення параметрів *pla*, *plb*, *h* та *kff*. За їх значеннями та числом *N* визначити: кількість елементів *fa* загальної факторної бази за формулою $fa = \exp\left( pla \cdot \frac{\sqrt{2}}{4} \sqrt{\ln N \cdot \ln\ln N} \right)$; базове значення розміру радіусу просіювання *fb* за формулою $fb = \exp\left( plb \cdot \frac{\sqrt{2}}{4} \sqrt{\ln N \cdot \ln\ln N} \right)$; границю гладкості B згідно зі значенням *fa*; граничне значення *ff* порядкового номера простого числа, що визначає множину можливих простих дільників *p* в остачах $y_k(X)$, показники степенів яких можуть перевищувати одиницю.

Обчислити значення логарифмів для всіх елементів ЗФБ. Дані запам’ятати в деякому масиві для подальшого використання.

Для всіх простих чисел, порядкові номери яких не перевищують *ff*, визначити їх степені, що не перевищують деякого вибраного значення, наприклад, границю гладкості B чи обмеження на тип даних. Дані запам’ятати (наприклад, в масиві mpb[*ff*]). Тоді при B < 300 для числа 2, порядковий номер якого в списку простих дорівнює одиниці, mpb[1] = 256, для числа 3 mpb[2] = 243 і т.д.

Лічильнику *k* присвоїти значення нуль.

2. $k = k + 1$.

3. У випадках, коли *k* ділиться на квадрат двох чи більше різних простих чисел, перейти до кроку 2.

4. Для числа *kN* виконати:

4.1. Сформувати множину елементів поточної факторної бази, до якої будуть віднесені такі прості $p$, що є елементами ЗФБ:

- прості $p$, для яких $(kN) \pmod p$ є квадратним лишком;
- прості $p$, що є дільниками $k$, якщо $k \pmod{p^2} > 0$.

У випадках, коли для деякого одного простого $p$, $k \pmod{p^2} = 0$, виключити таке $p$ з множини елементів поточної факторної бази.

4.2. Визначити число $pfa$ елементів поточної факторної бази. Якщо $(2 \cdot pfa / fa)^5 < 0.75$, перейти до кроку 2, а при $(2 \cdot pfa / fa)^5 \geq 0.75$ обчислити значення поточного (залежного від $k$) радіусу просіювання $pfb = fb \cdot (2 \cdot pfa / fa)^5$ та перейти до кроку 4.4.

4.4. Визначити $x_0 = \lfloor \sqrt{kN} \rfloor + 1$ та присвоїти значення: $xp = x_0$, $xm = x_0 - 1$, $yp = xp^2 - kN$ і $ym = kN - xm^2$. Визначити коефіцієнти розкладання $xp$, $xm$, $yp$ і $ym$ за основою 1000. Результати розкладання записати в масиви, наприклад, $xp0[]$, $xm0[]$, $yp0[]$ і $ym0[]$. Визначити перші 5 коефіцієнтів розкладання чисел $xp$, $xm$, $yp$ і $ym$ за основами степенів простих чисел, записаних в масиві mpb[$ff$] (кількість коефіцієнтів може розглядатися як параметр, а їх число 5 вибрано на основі чисельних експериментів). Результати розкладання записати в масиви, наприклад, $xpp[]$, $xmp[]$, $ypp[]$ і $ymp[]$.

4.5. Обчислити значення логарифму $lxp = \log(xp)$.

4.6. Для всіх простих з поточної факторної бази знайти корені рівняння

$$(y_k(X)) \pmod p = 0 \qquad (5)$$

користуючись алгоритмом Шенкса. Значення меншого з коренів запам'ятати в масиві, наприклад mx1[$f_p$], де $f_p$ – порядковий номер простого $p$ в списку простих.

5. $c$=0. Пробні $X = x_0$ та $X = x_0 - 1$ вважати елементами множини MV($h$). Перевірити чи будуть B-гладкими остачі $y_k(x_0)$ та $y_k(x_0 - 1)$.

6. Виділити дві підмножини з інтервалу просіювання: ($x_0$+$c$, $x_0$+$c$+$z$] та [$x_0$–$c$–$z$, $x_0$–$c$), де $z = \min(1000, (pfb - x_0 - c))$.

7. Для $t = 1 \div z$ присвоїти значення нуль елементам масивів $mzp[t]$ і $mzm[t]$ та знайти наближене значення логарифму $\log(y_k(x_0 + c + t)) \approx lxp + \log(2c + t) = mlp[t]$.

8. Для кожного з елементів $p$ поточної факторної бази визначити ті зі значень пробних $X = x_0 + c + t$ з підмножини ($x_0$+$c$, $x_0$+$c$+$z$], для яких має місце рівність (5), і для них додати значення логарифму від $p$, значення якого записано в p_log[$f_p$], до елементу масиву $mzp[t]$.

9. На основі порівняння значень $mzp[t]$ та $mlp[t]$ з урахуванням значення параметра $h$ визначити пробні $X$, що належать множині MV($h$).

10. Для $X \in$ MV($h$) перевірити чи існують дільники $p$ з показником степеня $s$ вище одиниці для остачі $y_k(X)$ серед простих чисел з поточної факторної бази, для яких $f_p \leq ff$. Якщо такі існують, то для кожного з таких $p$ при $X = x_0 + c + t$ до

елемента масиву $mzp[t]$ додати значення $(s\text{-}1)\cdot\text{p\_log}[f_p]$. Якщо в результаті виявиться, що

$$|mzp[t] - mlp[t]| < 0.1, \tag{6}$$

то $y_k(X)$ буде B-гладкою остачею.

11. Для кожного з елементів $p$ поточної факторної бази визначити ті зі значень пробних $X = x_0 - c - t$ з підмножини $[x_0–c–z, x_0–c)$, для яких має місце рівність (5), і для них додати значення логарифму від $p$, значення якого записано в $\text{p\_log}[f_p]$, до елементу масиву $mzm[t]$.

12. На основі порівняння значень $mzm[t]$ та $mlm[t]$ з урахуванням значення параметра $h$ визначити пробні $X$, що належать множині MV($h$).

13. Для $X \in$ MV($h$) і $X = x_0 - c - t$ перевірити чи існують дільники $p$ з показником степеня $s$ вище одиниці для остачі $y_k(X)$ серед простих чисел з поточної факторної бази, для яких $f_p \le ff$. Якщо такі існують, то для кожного з таких $p$ до елемента масиву $mzm[t]$ додати значення $(s\text{-}1)\cdot\text{p\_log}[f_p]$. Якщо в результаті виявиться, що

$$|mzm[t] - mlm[t]| < 0.1, \tag{7}$$

то $y_k(X)$ буде B-гладкою остачею.

14. Якщо число B-гладких перевищує $fa$, перейти до п. 16, а інакше до п. 15.

15. $c = c + z$. Якщо $c = pfb$, перейти до п. 2, а інакше до п. 6.

16. Діагоналізувати матрицю та знайти нульовий рядок. Якщо нульовому рядку відповідає тривіальний корінь рівняння $A^2 (\mathrm{mod}\, N) = B^2 (\mathrm{mod}\, N)$, де $A$ – це добуток ряду пробних значень $X$, а $B$ – добуток відповідних їм остач (3), замінити його іншим B-гладким, за наявності, а інакше перейти до кроку 2. Якщо ж отримано нетривіальний корінь, то вивести значення множників числа $N$ і закінчити роботу алгоритму.

При використанні алгоритму **A** отримано зниження часу знаходження достатньої кількості B-гладких для тієї ж множини значень $N$ для $m = 20 \div 30$ в 14-22 рази для значень параметрів $plb$ =1.4, $h$ = 0.7, $kff$ = 1.0 та значень $pla$ = 1.0, $pla$ = 0.95 і $pla$ = 0.9. Це підтверджує високу ефективність процедури попереднього просіювання.

При значеннях параметрів $pla$ 0.9÷0.94, $plb$ =1.4, h=0.7, $kff$ = 0.4÷0.6 для визначеної множини чисел порядку $10^m$, де $m$=20÷32, отримано значення коефіцієнту $C < 1$ в оцінці складності методу MQkS виду $O\left(\exp(C\sqrt{\ln N \ln\ln N})\right)$. У відомих оцінках обчислювальної складності методів методів QS та MPQS коефіцієнт $C \ge 1$. 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 MQkS та зменшується час пошуку B-гладких.

**Третій розділ** Присвячений методам зменшення обчислювальної складності вирішення задачі факторизації для окремих випадків чисел N а також питанням зниження необхідного розміру оперативної пам'яті при вирішенні матриці.

***Метод рішення матриці «на ходу» зі зменшеним розміром необхідного розміру оперативної пам'яті.*** В пропонованому алгоритмі методу, що реалізує вирішення матриці на ходу, використовується додатковий вектор *Vs*[*fa*+1], в якому фіксується послідовність перестановок стовпчиків матриці.

Пошук нульового вектора для матриці степенів представлені наступними кроками:

1. При появі нового B-гладкого числа, по вектору показників степенів *Vnew* його множників сформувати значення коефіцієнтів відповідного рядка *kv* матриці за правилом: одиниці дорівнюють тільки коефіцієнти, що відповідають непарним показникам степеня множника, а всі інші дорівнюють нулю.
2. Якщо всі елементи рядка *kv* матриці дорівнюють нулю, то перейти до пункту 4 (нульовий вектор знайдено), а інакше до п.3.
3. В рядку *kv* матриці знайти номер позиції *k0*, що відповідає першому ненульовому значенню. Якщо *Vs*[*k*0] = 0, присвоїти *Vs*[*k*0] = *kv* та перейти до п.1, а інакше до рядка *kv* матриці додати (по модулю два) рядок *Vs*[*k*0] і перейти до п.2.
4. Вияснити, чи отримане значення кореня не дорівнює *N*. Якщо ні, то задача факторизації вирішена, а інакше перейти до пункту 5.
5. Видалити з матриці інформацію про *B*–гладке. Перейти до пункту 1.

Аналіз ефективності проводився за декількома ознаками:

1. Кількість просіяних *X* для базового та модифікованого методу.
2. Загальний час виконання завдання факторизації.

Був розроблений додаток, що реалізує описаний алгоритм рішення матриці на ходу. На основі чисельних експериментів було встановлено, що в окремих випадках можливі прискорення в 10, 100 і більше разів по відношенню до базового методу QS, коли мало місце отримання нульового вектора значно раніше ніж були знайдені $L^a$+2 B-гладких числа, що передбачено в алгоритмі базового методу. Наведено такі приклади.

Встановлено також, що на основі вирішення матриці на ходу були виявлені випадки чисел, які вдалося факторизувати, а базовий алгоритм квадратичного решета (при стандартному інтервалі просіювання та розміру факторної бази) не зміг сформувати матрицю для отримання рішення. Серед 10000 чисел розміром $10^{13}$ модифікований алгоритм зміг зменшити кількість невдалих факторизацій з 686 випадків до 503.

***Метод вибору достатньої кількості B – гладких чисел.***

В пропонованому алгоритмі **MLB**, що реалізує вибір достатньої кількості B-гладких чисел при розмірі факторної бази *fa*, використовуються додатковий вектор *Vf*[*fa*+1] та вектори *Ve*[*fa*+1], *VB*[*fa*+2], *VM*[*fa*+2].

Вектор *Ve* – це інформація про показники степенів отриманого нового B – гладкого числа. В клітинці *t* вектора *VB* міститься інформація про значення числа з інтервалу просіювання ($-L^b$, $L^b$) на основі якого отримано B – гладке число з номером *t*. Для B – гладкого числа номер *t* в клітинці *t* вектора *VM* задається порядковий номер максимального за значенням дільника з непарним показником степеня.

В кожній клітинці *k* вектора *Vf* спочатку присвоюється значення *k* + 2. А при кожному отриманні B – гладкого числа визначається порядковий номер *s* максимального за значенням дільника з непарним показником степеня та від всіх елементів вектора *Vf*, номер яких більший або рівний *s*, зменшується їх значення на одиницю. Якщо при цьому виявиться, що значення в якійсь з клітинок вектора *Vf* стане рівним нулю, то серед отриманих B-гладких чисел буде *s* + 2 таких, що утворять матрицю СЛАР з числом рівнянь *s* + 2 при *s* + 1 невідомому, що забезпечить отримання нульового рядка.

***Умовно B-гладкі числа та їх використання для зниження обчислювальної складності процесу факторизації великих чисел.***

На основі чисельних експериментів було встановлено що в ряді випадків пришвидшити знаходження достатньої множини B-гладких чисел можна на основі використання умовно B-гладких чисел, тобто таких що $y_k(x) = \prod_{i=0}^{F} p_i^{a_i} * c_x^2$, де $p_i$ - просте з факторної бази, $c_x$ - просте, або добуток простих, більших за границю гладкості B.

На основі проведених чисельних експериментів показано, що використання умовно B-гладких чисел у випадку базового алгоритму квадратичного решета зменшує число невдалих факторизацій з 11% до 3%. При цьому можливі випадки, коли на основі використання умовно B-гладких та методу діагоналізації на ходу велике число може бути факторизовано значно швидше, ніж будуть сформовані *fa*+2 рядки матриці.

Застосування умовно B-гладкі дозволяє знаходити рішення для деяких N, навіть коли розмір факторної бази дорівнює нулю. Тому такий метод можна вважати подальшим розвитком методу Ферма і він є певного роду переходом від методу Ферма до методу квадратичного решета. На відміну від методу Ферма метод використовує не тільки квадрати $X^2 - N$ які є додатними а і від'ємні значення, при цьому для факторизації достатньо не більше двох умовно B-гладких чисел. Наведено приклади.

**В четвертому розділі** вирішується ряд завдань, пов’язаних з реалізацією методу MQkS в залежності від обраної архітектури апаратно-програмних засобів.

Застосування графічних карт може дати суттєве прискорення у роботі алгоритмів факторизації. Популярність і інтенсивне розвиток технології CUDA, повна апаратна підтримка цілочисельних та побітових операцій, висока ступінь паралелізму розрахунків, наявність своєї внутрішньої пам'яті, яка володіє більш високою швидкодією у порівнянні з ОЗУ – причини застосування архітектури CUDA.

Але існують апаратні обмеження на типи даних та об’єм пам’яті, що необхідно враховувати про реалізації чисельних методів.

Запропонований метод MQkS є гнучким по відношенню до можливостей апаратно-програмних засобів. В залежності від наявного обсягу пам’яті та розрядності базових типів даних у методі MQkS передбачається ряд параметрів.

Параметр *pla* регулює розмір ЗФБ, яка визначається як $fa = \left( \exp\left( \frac{\sqrt{2}}{4} \sqrt{\ln N \cdot \ln \ln N} \right) \right)^{pla}$ на всіх етапах факторизації та розмір матриці на останньому етапі факторизації;

При використанні параметра *h* на етапі попереднього просіювання використовуються тільки перші степені дільників $y_k(X)$, та немає потреби знаходження квадратних лишків для всіх степенів елементів факторної бази і їх подальшого використання;

Параметр *kff* дозволяє явно визначити кількість простих чисел, що будуть використані для пошуку дільників $y_k(X)$, показник степеня яких перевищує одиницю. За рахунок вибору *kff* можна регулювати обсяг пам’яті який використовується для роботи з процесорами графічних карт.

Для чисел N розміром $2^{1024}$ розмір факторної бази для стандартного методу квадратичного решета складає $30*10^9$. Тобто один рядок матриці буде займати як мінімум 30 GB пам’яті. Для методу MQkS розмір факторної бази визначаться на основі значення параметру *pla* а може бути зменшене до 100 і більше разів. А якщо ж розмір факторної бази становить $10^8$, то необхідно зберігати до 2GB даних.

В ході виконання процедури попереднього просіювання до графічних карт передається інформація про значення X які пройшли попереднє просіювання, розміром до 62 kB, що відповідає обмеженням на доступний обсяг пам’яті графічних карт

При обмеженнях пам’яті у графічних картах 1.5 Gb, алгоритм дозволяє завантажити одній графічній карті до 24200 варіантів *k*.

Тому пропонується розбити процес факторизації на чотири етапи, кожен з яких буде виконуватись на різних апаратних складових обчислювальної системи:

1. введення числа N, обчислення розміру факторної бази та інтервалу просіювання – головний комп'ютер, управління процесом обчислень;
2. операції попереднього просіювання (потребують великої кількості пам'яті) вузол кластера для кожного з *k*;
3. кінцеве просіювання із застосуванням графічних карт (обсяг пам'яті обмежено через обмеження архітектури);
4. рішення матриці – супер-комп'ютер.

У випадку коли комп'ютерна система передбачає прямий зв'язок із суперком'ютером, можна безпосередньо після кожного знайденого B-гладкого числа передавати інформацію на суперком'ютер. Тоді доцільно використовувати метод рішення на ходу. Проте, якщо такої можливості немає, тоді є смисл використання методу достатньої кількості B-гладких чисел, який несутєво збільшує необхідний обсяг оперативної пам'яті та обчислювальну складність, проте в ряді випадків дозволяє набагато швидше вирішити задачу факторизації.

## ВИСНОВКИ

У дисертаційній роботі вирішена науково-практична задача розробки обчислювальних методів факторизації на основі методів QS та MPQS, які можна використовувати в сучасних апаратно програмних комплексах, що забезпечило зниження обчислювальної складності в порівнянні з уже існуючими методами QS та MPQS при вирішенні завдань криптоаналізу RSA.

Основні наукові і практичні результати роботи полягають у наступному:

1. Розроблено метод множинного квадратичного *k*-решета (MQkS), в якому для пошуку B-гладких остач використовуються остачі $y_k(X) = X^2 - kN$, що при більшості значень *k* забезпечує пошук B-гладких серед всіх пробних $X = X_0 + x = \lfloor \sqrt{N} + 1 \rfloor + x$ в єдиному інтервалі просіювання, в якому, на відміну від методів QS та MPQS:

- використовується загальна факторна база (ЗФБ), утворена всіма найменшими простими числами починаючи з 2, кількість яких $fa = \left( \exp\left( \frac{\sqrt{2}}{4} \sqrt{\ln N \cdot \ln \ln N} \right) \right)^{pla} = \left( L^a \right)^{pla}$, де, $pla \in [0.5, 1.5]$ – параметр, а при кожному зі значень *k* з елементів ЗФБ формується поточна факторна база;
- розмір радіусу просіювання $fb = \left( L^a \right)^{plb}$, де $plb \in [0.5, 4]$ – параметр;
- на етапі просіювання реалізується попереднє просіювання пробних *X* на основі використання сигнальних остач $y^*(X)$, що є добутками перших степенів дільників $y_k(X)$ з числа елементів ЗФБ, при якому до множини відсіяних *X* відносяться ті, для яких виконана умова $\log\left(y_k^*(X)\right) < h \cdot \log\left(y_k(X)\right)$, де $h \in [0, 1]$ – параметр;

- при просіюванні пробних $X$, які не були відсіяні, пошук дільників остач $y_k(X)$, показник степеня яких може перевищувати одиницю, здійснюється для простих чисел з поточної факторної бази за умови, що для порядкового номера $f_p$ простого $p$ у списку простих чисел виконана умова $f_p \le ff = (L^a)^{kff}$, де $kff \in [0, 1]$ – параметр, при виборі якого можливе врахування даних про обмеження на обсяг пам'яті та доступні стандартні типи даних апаратних засобів;
- при пошуку нульового рядка матриці, елементи якої дорівнюють одиниці для непарних показників степеня дільників B-гладких чисел при рівних нулю інших значеннях, за рахунок перенумерації стовпчиків замість двох матриць з числом стовпчиків, що дорівнює $fa$, використовується одна, за рахунок чого розмір необхідної пам'яті суперкомп'ютера можна скоротити вдвічі.

При значеннях параметрів $pla$ 0.9÷0.94, $plb$ =1.4, $h$=0.7, $kff$ = 0.4÷0.6 для визначеної множини чисел порядку $10^m$, де $m$=20÷32, отримано значення коефіцієнту $C < 1$ в оцінці складності методу MQkS виду $O\left(\exp(C\sqrt{\ln N \ln\ln N})\right)$. У відомих оцінках обчислювальної складності методів методів QS та MPQS коефіцієнт $C \ge 1$. 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. Виявлені випадки отримання нульового стовпчика для матриці, що формується на основі показників степенів дільників B-гладких, та запропоновано метод діагоналізації матриці «на ходу», що в окремих випадках може забезпечити розкладання криптомодуля $N$ на множники раніше ніж будуть знайдені $fa$ + 2 B-гладкі остачі $y_k(X)$ незалежно від величини числа $N$. Даний результат може бути використаний для методів MQkS, QS, та MPQS.

3. Запропоновано метод визначення достатньої кількості B - гладких чисел, при використанні яких можна сформувати матрицю за показниками степенів дільників B-гладких, де можливими є випадки формування достатньої кількості B - гладких для отримання нульового рядка раніше, ніж буде знайдено $fa$ + 2 B-гладких остач $y_k(X)$.

4. Встановлено, що серед остач $y_k(X)$ існуть такі, 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. Такі числа названо умовно B-гладкими та показано, що існують випадки, коли на основі їх використання 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.

5. Запропоновано алгоритм реалізації методу MQkS на апаратно-програмних засобах, які включають суперкомп'ютер, 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.

6. Розроблено рекомендації стосовно використання розроблених методів в залежності від можливості апаратних засобів та загальна структура апаратно-програмних засобів при оцінці криптографічної стійкості RSA-алгоритму.

Таким чином, розроблені обчислювальні методи та запропоновані науково-технічні рішення в сукупності дозволяють підвищити швидкодію апаратно-програмних і програмних засобів, що використовуються при оцінюванні криптостійкості АКА RSA. Це має важливу наукову й практичну спрямованість при удосконаленні існуючих та створенні нових засобів для проведення тематичних досліджень для допуску до експлуатації КЗІ, що використовують АКА.

Результати роботи використані при виконанні НДР «Розвиток методів зниження енергоспоживання обчислювальних систем за рахунок оптимізації обробки масивів даних (шифр – ФРІСК)», (д/р № 0114U000879), та, 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, та використовуються в навчальному процесі в Інститут спеціального зв’язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського”.

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ


1. Факторизация числа N= pq при простых p и q методом дискретного логарифмирования. / ВН Мисько, СД Винничук, АВ Жилин. // Электронное моделирование . – 2013. – № 5 (35). – С. 3-10.
2. Ускорение метода Ферма методом прореживания с использованием нескольких баз. /В.М. Міська. // Журнал «Безпека інформації». Ukrainian Scientific Journal of Information Security. – 2015. – № 1 (21). – С. 64-68. DOI: 10.18372/2225-5036.21.8310
3. Удосконалення методу квадратичного решета на основі використання розширеної факторної бази та формування достатньої кількості B - гладких чисел. / В.М. Міська, С.Д. Винничук. // Збірник "Information technology and security". – 2017. – том. 5. выпуск. 2 (9). – С. 67-75.
4. Прискорення методу квадратичного решета на основі використання додаткового пошуку B-гладких чисел. / Міська В.М. // Моделювання та інформаційні технології. Збірник наукових праць. – 2017. – №78. – С. 51-57.

5. Acceleration analysis of the quadratic sieve method based on the online matrix solving. / V. Misko, S. Vynnychuk. // Eastern-European journal of Enterprise technologies. – 2018. – №10 (2). – С. 33-38. DOI: 10.15587/1729-4061.2018.127596
6. “Прискорення методу квадратичного решета на основі використання умовно B-гладких чисел” / Міський В.М. // Міжнародний науково–технічний журнал. Системні дослідження та інформаційні технології. – 2018. – №1. – С. 99-106. DOI: 10.20535/SRIT.2308-8893.2018.1.08
7. “Метод множинного квадратичного k-решета цілочисельної факторизації.” / В.М. Міський, С.Д. Винничук. // Електронне моделювання. – 2018. – №5 (40) С. 3-26. DOI: https://doi.org/10.15407/emodel.40.05.003
8. Просіювання пробних значень в методі множинного квадратичного k-решета на основі сигнальних остач. / С.Д. Винничук, В.М. Міський. // Безпека інформації. – 2019. – №1 (25). – С. 45-52. DOI: 10.18372/2225-5036.25.13446
9. “Метод множинного квадратичного k-решета з використанням сигнальних остач при просіюванні пробних значень.” / В.М. Міський, С.Д. Винничук. // Електронне моделювання. – 2019. – №2 (41) С. 3-22. DOI: https://doi.org/10.15407/emodel.41.02.003
10. “Ускорение метода Ферма факторизации чисел вида n = pq, где p и q простые, методом прореживания.” / В.М. Мисько. // Матеріали XXXIV Науково-технічної конференції «Моделювання» ІПМЕ ім. Г.Є. Пухова НАН України. 13-14 січня 2015 року. – тези доп. – м. Київ. – С.7.
11. “Ускорение метода Ферма факторизации чисел вида n = pq, где p и q простые, методом прореживания с использованием нескольких баз. ” / С.Д. Винничук, В.М. Міський. // Матеріали XXXVI Науково-технічної конференції «Моделювання» ІПМЕ ім. Г.Є. Пухова НАН України. 12-13 січня 2016 року. – тези доп. – м. Київ. – С.22.
12. “Прискорення методу квадратичного решета на основі використання розширеної факторної бази та формування достатньої кількості B-гладких чисел” / В.М. Міський. // ІІІ Міжнародна науково-практична конференція "Інформаційна безпека та комп’ютерні технології" 19-20 квітня 2018 року.: тези доп. – м. Кропивницький., – С. 106-108.
13. “Прискорення методу квадратичного решета на основі пошуку додаткових B-гладких чисел.” / В.М. Міський // Матеріали VI заочної наукової конференції «Наукові підсумки 2017 р», 13.11.2017. Науковий журнал «ScienceRise». – 2017. – №12(41). м. Харків. – С. 67-71. DOI: 10.15587/2313-8416.2017.118298
14. «Прискорення методу квадратичного решета на основі рішення матриці на ходу.» / В.М. Міський // Програма І Міжнародної науково-практична конференції “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS). 05-06 квітня 2018 р,: тези доп. – К., – С. 272-274.

15. «Прискорення методу квадратичного решета на основі рішення матриці на ходу». / В.М. Міська // Щорічна науково-технічна конференція молодих вчених та спеціалістів ІПМЕ ім. Г.Є. Пухова НАН України. 16 травня 2018 року, м. Київ. ,: тези доп. – К., – С. 29-30.
16. Множинне Квадратичне К-решето (MQKS). / С.Д. Винничук. В.М. Міська // Матеріали VI міжнародної наукової конференції «Моделювання-2018». 12-14 вересня 2018 р.: тези доп. – К., – С. 207-210 .
17. Множинне квадратичне k-решето факторизації чисел. / С.Д. Винничук В.М. Міська // Матеріали науково-практичної конференції «Сучасні інформаційні технології та кібербезпека», 15-16 листопада 2018р.: тези доп. – К., – С. 194-197.
18. Метод множинного квадратичного k-решета з використанням сигнальних остач при просіювання пробних значень. / В.М. Міська, С.Д. Винничук // XII Міжнародна науково-практична конференція «Комп'ютерні системи та мережеві технології» 28 –30 березня 2019 року.: тези доп. – К., – С. 27-28.

## АНОТАЦІЯ

**Міська В.М. Обчислювальні методи на основі квадратичного решета при криптоаналізі RSA алгоритму апаратно-програмними засобами.** – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 01.05.02 – математичне моделювання та обчислювальні методи. – Інститут проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України, Київ, 2019.

Дисертаційна робота Міська В.М. присвячена удосконалення існуючих та розробці 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.

Новими науковими результатами, отриманими в дисертаційній роботі, є новий метод множинного квадратичного *k*-решета (MQkS), в якому для пошуку B-гладких остач використовуються остачі $y_k(X)=X^2-kN$, що при більшості значень *k* забезпечує пошук B-гладких серед всіх пробних $X = X_0 + x = \left\lfloor \sqrt{N} + 1 \right\rfloor + x$ в єдиному інтервалі просіювання без обмежень на *x*. В методі передбачено використання

- загальної факторної бази, утворена всіма найменшими простими числами починаючи з 2, кількість яких визначається згідно зі значенням параметра *pla*, а при кожному зі значень *k* з елементів ЗФБ формується поточна факторна база;

- розміру радіусу просіювання визначається згідно зі значенням параметра *plb*;
- попереднього просіювання пробних $X$ на основі використання сигнальних остач $y^*(X)$, що є добутками перших степенів дільників $y_k(X)$ з числа елементів ЗФБ, при якому до множини відсіяних $X$ відносяться ті, для яких виконана умова $\log\left(y_k^*(X)\right) < h \cdot \log\left(y_k(X)\right)$, де $h \in [0, 1]$ – параметр;
- пошук B-гладких за умови, що для дільників остач $y_k(X)$, показник степеня яких може перевищувати одиницю, здійснюється для простих чисел з поточної факторної бази, які не перевищують максимальне значення, що визначається згідно зі значенням параметра *kff* що дозволяє враховувати обмеження на обсяг пам'яті та доступні стандартні типи даних апаратних засобів.

Запропонований метод є гнучким по відношенню до можливостей апаратно-програмних засобів, що може бути реалізовано на основі вибору параметрів *pla*, *plb*, *kff*, та *h*. Розроблено рекомендації стосовно використання розроблених методів в залежності від можливості апаратних засобів та загальна структура апаратно-програмних засобів при оцінці криптографічної стійкості RSA-алгоритму.

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 $fa + 2$ B-гладкі остачі $y_k(X)$ незалежно від величини числа $N$.

Запропоновано алгоритм реалізації методу MQkS на апаратно-програмних засобах, які включають суперкомп'ютер, 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.

Результати роботи дозволяють підвищити швидкодію апаратно-програмних засобів, які використовуються для проведення криптоаналізу RSA криптоалгоритму.

**Ключові слова:** факторизація, багаторозрядні числа, RSA, QS, MPQS, MQkS, умовно B-гладкі, на ходу, достатня кількість B-гладких, графічні карти.

## АННОТАЦИЯ

**Мисько В.Н. Вычислительные методы на основе квадратичного решета при криптоанализе RSA алгоритма аппаратно-программными средствами.** – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 01.05.02 - математическое моделирование и вычислительные методы. - Институт проблем моделирования в энергетике им. Г.Е. Пухова НАН Украины, Киев, 2019.

Диссертационная работа Мисько В.М. посвящена совершенствованию существующих и разработке новых современных вычислительных методов факторизации на основе методов QS и MPQS, которые можно использовать в современных аппаратно-программных комплексах, что обеспечит снижение вычислительной сложности по сравнению с уже существующими методами QS и MPQS при решении задачи криптоанализа RSA алгоритма.

Новыми научными результатами, полученными в диссертационной работе, является новый метод множественного квадратичного k-решета (MQkS), в котором для поиска B-гладких остатков используются остатки $y_k(X)=X^2-kN$, что при большинстве значений $k$ обеспечивает поиск B-гладких среди всех пробных $X = X_0 + x = \left\lfloor \sqrt{N} + 1 \right\rfloor + x$ в едином интервале просеивания без ограничений на $x$. В методе предусмотрено использование

– общей факторной базы, образованная всеми наименьшими простыми числами начиная с 2, количество которых определяется в соответствии со значением параметра *pla*, а при каждом из значений $k$ из элементов общей факторной базы формируется текущая факторная база;
– размера радиуса просеивания определяется согласно значению параметра *plb*;
– предварительного просеивания пробных $X$ на основе использования сигнальных остатков $y^*(X)$. Которые являются произведениями первых степеней делителей $y_k(X)$, из числа элементов общей факторной базы, при которых к множеству отсеянных $X$ относятся те, для которых выполнено условие $\log\left(y_k^*(X)\right) < h \cdot \log\left(y_k(X)\right)$, где $h \in [0, 1]$ - параметр;
– поиск B-гладких при условии, что для делителей остаток $y_k(X)$, показатель степени которых может превышать единицу, осуществляется для простых чисел с текущей факторной базы, которые не превышают максимальное значение. Такое значение определяется согласно значению параметра *kff*, что позволяет учитывать ограничения на объём памяти и доступные стандартные типы данных аппаратных средств.

Предложенный метод является гибким по отношению к возможностям аппаратно-программных средств, что может быть реализовано на основе выбора параметров *pla*, *plb*, *kff*, и *h*. Разработаны рекомендации по использованию разработанных методов в зависимости от возможности аппаратных средств и общая структура аппаратно-программных средств, при оценке криптографической стойкости RSA-алгоритма.

Предложен метод диагонализации матрицы «на ходу» и метод определения достаточного количества B - гладких чисел что в отдельных случаях может обеспечить разложение криптомодуля $N$ на множители раньше чем будут найдены $fa + 2$ B-гладких остатков $y_k(X)$ независимо от величины числа N.

Предложен алгоритм реализации метода MQkS на аппаратно-программных средствах, которые включают суперкомпьютер, кластеры и графические процессоры, в которых учитываются ограничения на стандартные типы данных и объем доступной памяти, а выполнение арифметических операций с многоразрядными числами заменяются операциями с числами типа long (или long long) и double.

Результаты работы позволяют повысить быстродействие аппаратно-программных средств, используемых для проведения криптоанализа алгоритма RSA.

**Ключевые слова:** факторизация, многоразрядные числа, RSA, QS, MPQS, MQkS, условно B-гладкие, на ходу, достаточное количество B-гладких, графические карты.

## ANNOTATION

**Misko V.M. Computational methods based on a quadratic sieve for cryptanalysis of RSA algorithm using hardware and software solution.** – As the manuscript

Thesis for the degree of candidate of technical sciences in the specialty 01.05.02 - mathematical modeling and computational methods - Pukhov Institute for Modelling in Energy Engineering of the NAS of Ukraine, Kyiv, 2019.

Thesis work Misko V.M. dedicated to improving existing and developing new computational factorization methods based on QS and MPQS methods that can be used in modern hardware and software solutions, which will reduce the computational complexity compared to the existing QS and MPQS methods in solving the cryptanalysis of RSA algorithm.

The new scientific results obtained in the thesis are the new multiple quadratic k-sieve method (MQkS), in which the residues $y_k(X)=X^2-kN$ are used to search for B-smooth residues, which for most $k$ values help to find B-smooth among all $X = X_0 + x = \left\lfloor \sqrt{N} + 1 \right\rfloor + x$ in a single sieving interval without restrictions on $x$. The method provides for the use of

- the total factor base formed by all the smallest prime numbers starting from 2, the number of which is determined in accordance with the value of the parameter *pla*, and for each of the values of $k$, the current factor base is formed from the elements of the CFB;
- radius of the sieving size is determined according to the value of the parameter *plb*;
- pre-sieving $X$ valuse based on the use of signal residues $y^*(X)$. Which are products of the first degrees of the divisors $y_k(X)$, from among the elements of the CFB, in which the set of sieved X includes those for which the condition $\log\left(y_k^*(X)\right) < h \cdot \log\left(y_k(X)\right)$ is satisfied, where $h \in [0, 1]$ is a parameter;

– B-smooth search, provided that for divisors the remainder $y_k(X)$, the exponent of which may exceed one, is performed for primes from the current factor base that do not exceed the maximum value. This value is determined according to the value of the *kff* parameter, which allows to take into account the limitations on the amount of memory and the available standard data types of hardware.

The proposed method is flexible with respect to the capabilities of hardware and software, which can be implemented based on the choice of the parameters *pla, plb, kff,* and *h*. Developed recommendations on the use of the developed methods, depending on the capabilities of the hardware and the overall structure of hardware and software, when evaluating the cryptographic strength of the RSA-algorithm.

A method of diagonalization of the matrix “on the fly” and a method for determining a sufficient number of B - smooth numbers are proposed, which in some cases can provide a decomposition of a crypto module N into factors before *fa* + 2 B smooth residues $y_k(X)$ are found, regardless of the value of N.

An algorithm for implementing the MQkS method on hardware and software tools, which include a supercomputer, clusters and graphics processors, which take into account restrictions on standard data types and available memory, is proposed, and arithmetic operations with multi-digit numbers are replaced by operations with numbers such as long (or long long ) and double.

The results of the work make it possible to increase the speed of the hardware and software solution used to perform cryptoanalysis of the RSA algorithm.

**Keywords:** factorization, multi-digit numbers, RSA, QS, MPQS, MQkS, conditionally B-smooth, on the fly, sufficient number of B-smooth, graphics cards.