НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

«До захисту допущено»
В.о. завідувача кафедри
_____ Михайло САВЧУК
«__» _____ 2021 р.

Дипломна робота

на здобуття ступеня бакалавра

зі спеціальності: 113 Прикладна математика
на тему: **«Побудова атаки з використанням структури простих чисел на RSA подібні криптосистеми зі складеним модулем»**

Виконала: студентка 4 курсу, групи ФІ-73
Мазур Анастасія Андріївна

Керівник: к.ф.-м.н., ст. викладач Фесенко А.В. _____

Консультант: _ _____

Рецензент: к.т.н., доцент Стьопочкіна І.В. _____

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____

Київ — 2021

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра математичних методів захисту інформації

Рівень вищої освіти — перший (бакалаврський)
Спеціальність (освітня програма) — 113 Прикладна математика,
ОПП «Математичні методи криптографічного захисту інформації»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри
_____ Михайло САВЧУК
«__» _____ 2021 р.

ЗАВДАННЯ
на дипломну роботу

Студент: Мазур Анастасія Андріївна

1. Тема роботи: «*Побудова атаки з використанням структури простих чисел на RSA подібні криптосистеми зі складеним модулем*»,

керівник: к.ф.-м.н., ст. викладач Фесенко А.В.,

затверджені наказом по університету №__ від «__» _____ 2021р.

2. Термін подання студентом роботи: 4 червня 2021р.

3. Вихідні дані до роботи: *опубліковані джерела за тематикою дослідження*

4. Зміст роботи: *Досліджено криптосистему RSA та її модифікації; вдосконалено атаку з використанням структури простих чисел на криптосистему RSA та побудовано атаки на її модифікації*

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо): *«Презентація доповіді»*

6. Дата видачі завдання: 10 вересня 2020 р.

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання	Примітка
1	Узгодження напряму дослідження із науковим керівником	01 вересня -15 вересня 2020 р.	Виконано
2	Огляд опублікованих джерел за тематикою дослідження	15 вересня 2020 р. - 08 січня 2021 р.	Виконано
3	Узгодження теми роботи із науковим керівником	08 січня - 05 лютого 2021 р.	Виконано
4	Дослідження атаки з використанням структури простих на криптосистему RSA	05 лютого - 19 лютого 2021 р.	Виконано
5	Покращення атаки з використанням структури простих на криптосистему RSA	19 лютого - 05 березня 2021 р.	Виконано
6	Побудова атаки з використанням структури простих чисел на криптосистему $PP - RSA$	05 березня - 02 квітня 2021 р.	Виконано
7	Побудова атаки з використанням структури простих чисел на криптосистему $GPP - RSA$	02 квітня - 07 травня 2021 р.	Виконано
8	Обчислення оцінки кількості простих чисел, які використовуються побудованими атаками	07 травня - 28 травня 2021 р.	Виконано
9	Оформлення пояснювальної записки до роботи	травень 2021 р.	Виконано

Студент _____ Мазур А.А.

Керівник _____ Фесенко А.В.

РЕФЕРАТ

Кваліфікаційна робота містить: 56 стор., 63 джерела.

Метою роботи є дослідження стійкості RSA-подібних криптосистем зі складеним модулем до атаки з використанням часткового знання щодо простих чисел модуля.

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є стійкість RSA-подібних криптосистем зі складеним модулем до атаки з використанням структури простих чисел та наймолодших значущих бітів.

У ході дослідження зроблено огляд криптосистеми RSA та її модифікацій. Розглянуто наявні атаки на криптосистему RSA та на RSA-подібні криптосистеми.

Результатами роботи є покращення наявної атаки на криптосистему RSA. Досліджено криптосистеми $PP - RSA$ та $GPP - RSA$, які є модифікаціями криптосистеми RSA. Побудована атака з використанням структури простих чисел на криптосистему $PP - RSA$ та обчислена оцінка її складності. Побудована атака з використанням структури простих чисел на криптосистему $GPP - RSA$ та обчислена оцінка її складності. Обчислена оцінка кількості простих чисел спеціального вигляду, які використовуються у запропонованих атаках.

RSA, RSA-ПОДІБНІ КРИПТОСИСТЕМИ, АТАКА З ЧАСТКОВИМ ЗНАННЯМ КЛЮЧА

ABSTRACT

The thesis contains: 56 pages, 63 sources.

The purpose of work is analyzing the security of the RSA-type cryptosystems with a composed module to attack using partial knowledge of module's prime factors.

The object is information processes in cryptographic protection systems.

The subject is the resistance of RSA-type cryptosystems with a composed module to attack using special-structured primes and the least significant bits.

The thesis reviews the cryptosystem RSA and its modifications. Existing attacks on the RSA cryptosystem and on RSA-type cryptosystems are considered.

The result of work is to improve the existing attack on the RSA cryptosystem. Investigated $PP - RSA$ and $GPP - RSA$ cryptosystems, which are a modification of the RSA cryptosystem. Constructed attack using the special-structured primes on the $PP - RSA$ cryptosystems and calculated estimate of the complexity of the proposed attack. Constructed attack using the special-structured primes on the $GPP - RSA$ cryptosystems and calculated estimate of the complexity of the proposed attack. Estimate of the special-structured primes, which are used in the proposed attacks, is calculated.

RSA, RSA-TYPE CRYPTOSYSTEMS, PARTIAL KEY EXPOSURE ATTACK

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

НСД(a,b) — найбільший спільний дільник чисел a та b.

НСК(a,b) — найменше спільне кратне чисел a та b.

$\phi(n)$ — функція Ейлера

mod — остача від ділення

$o(\cdot)$ — нотація Ландау (о-маленьке)

$O(\cdot)$ — нотація Ландау (О-велике)

$L_n[\alpha,\, c] = exp((c + o(1))(log_2^{\alpha} n \cdot log_2(log_2^{1-\alpha} n)))$

$\mathbb{Z}_+$ — множина цілих додатних чисел

$\mathbb{Z}_n$ — множина цілих чисел від 0 до $n - 1$

$\mathbb{Z}_n^*$ — множина цілих чисел від 0 до $n - 1$, які є взаємно простими з n

$min(a, b)$ — функція, яка повертає мінімум з двох значень a та b.

$max(a, b)$ — функція, яка повертає максимум з двох значень a та b.

$\|x\|$ — бітова довжина числа x

$ln(\cdot)$ — натуральний логарифм

ВСТУП

Актуальність дослідження. Поява асиметричної криптографії дозволила вирішити багато проблем захисту інформації, зокрема: передача секретних ключів, автентифікація, безпечне зберігання паролів. Криптосистема RSA на сьогоднішній день є найпопулярнішим асиметричним криптопримітивом. Вона використовується в багатьох криптографічних протоколах, таких як: TLS, PGP, $IPSEC$, $SILC$, SSH [1], а також в схемах електронного цифрового підпису. Одним з критичних параметрів криптосистеми є швидкість розшифрування, а також розмір ключів. Задля підвищення ефективності криптосистеми почали з'являтися модифікації, які використовують алгоритми RSA, але з іншими модулями. Криптосистеми $PP-RSA$ та $GPP-RSA$ - деякі з таких модифікації, які дозволяють значно пришвидшити розшифрування, а також використовувати прості числа меншої довжини для генерування надійного ключа. Тому дослідження стійкості таких криптосистем є актуальною задачею, і для забезпечення надійності побудова кожної з них повинна враховувати наявні атаки.

Метою дослідження є дослідити стійкість RSA-подібних криптосистем зі складеним модулем до атаки з використанням часткового знання щодо простих чисел модуля.

Для досягнення мети необхідно вирішити такі завдання:

1) дослідити криптосистему RSA та її модифікації;

2) зробити огляд наявних атак на криптосистему RSA та її модифікації;

3) детально дослідити атаку з використанням структури простих на криптосистему RSA;

4) побудувати атаку з використанням структури простих чисел на криптосистему $PP-RSA$ та обчислити оцінку її складності;

5) побудувати атаку з використанням структури простих чисел на

криптосистему $GPP - RSA$ та обчислити оцінку її складності;

6) обчислити оцінку кількості простих чисел, які використовуються побудованими атаками.

Об'єктом дослідження є інформаційні процеси в системах криптографічного захисту.

Предметом дослідження є стійкість RSA-подібних криптосистем зі складеним модулем до атаки з використанням структури простих чисел та наймолодших значущих бітів.

При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи лінійної та абстрактної алгебри, комбінаторного аналізу, теорії складності алгоритмів.

Наукова новизна отриманих результатів полягає у покращені атаки на криптосистему RSA; побудові нової атаки на криптосистему $PP - RSA$ та криптосистему $GPP - RSA$ з використанням наймолодших значущих біт; отриманні оцінок складності запропонованих атак; обчисленні оцінки кількості простих чисел спеціального виду.

Практичне значення результатів полягає у створенні рекомендіцій щодо вибору секретних параметрів криптосистем $PP - RSA$ та $GPP - RSA$.

1 ТЕОРЕТИЧНІ ВІДОМОСТІ

У даному розділі розглядається криптосистема RSA та відомі атаки, які побудовані на цю криптосистему. Також розглядаються різні модифікації криптосистеми RSA, які дозволяють або пришвидшити розшифрування або побудувати більш стійку криптосистему до різного роду атак, використовуючи ідею RSA. Стійкість більшості описаних криптопримітивів ґрунтується на складності задачі факторизіції. На сьогоднішній день найкращі класичні алгоритми, які розв'язують задачу факторизіції, мають субекспоненційну складність. Однак, дуже багато атак з поліноміальною складністю побудовано на криптосистему RSA та її модифікації з використанням різних методів та припущень щодо відкритої експоненти, секретної експоненти та секретних ключів.

1.1 Опис криптосистеми RSA

У 1978 році Р. Рівест, А. Шамір та Л. Адлеман опублікували статтю [2] у якій запропоновано односторонню функцію з секретом, но основі якої авторами було побудовану криптосистему RSA. Для шифрування та розшифрування використовується функція піднесення у степінь e за модулем $n = pq$, де p та q різні прості числа приблизно однакової бітової довжини, які є секретними ключами криптосистеми. Число e - відкритий ключ, від нього вимагається: $1 < e < \phi(n)$ та НСД$(e, \phi(n)) = 1$ - це потрібно для того, щоб існувало обернене за модулем $\phi(n)$ число $d = e^{-1} \pmod{\phi(n)}$ - ще один секретний ключ. Швидкість шифрування та розшифрування при відомих e та d відповідно можна оцінити у кількості операцій множення та ділення. Якщо використовувати схему Горнера піднесення до степені, то кількість кожної з двох операцій не перевищує $2log_2e$. Зрозуміло, що для більшої

ефективності алгоритму зашифрування, e повинен бути якомога меншим, а значить найкраще використовувати відкритий ключ $e = 3$. Однак, було побудовано багато атак на криптосистему з відкритою експонентною 3, наприклад у роботах: [3], [4]. Зокрема Д. Коперсміт, М. Франклін, Ж. Патарін та М. Рейтерт у [5] показали що, якщо $e = 3$, то це дозволяє знайти відкриті тексти за відомими шифротекстами за умови, що два відкритих тексти зашифровані на одному відкритому ключі (e,n) та зв'язані між собою деяким лінійним відношенням. Для пришвидшення розшифрування або генерування цифрового підпису теж було б краще використовувати невеликий секретний ключ d, адже оцінки складності тут такі ж самі як і для шифрування. Але у 1990 році М. Вінер описав атаку, яка дозволяє знайти d за поліноміальний час, за умови що $p < q < 2p$ та $d < \frac{1}{3}(pq)^{\frac{1}{4}}$ [6]. Потім у 2000 році Д. Боне та Г. Дерфи у [7] вперше покращили оцінку, отримавши, що при $d < (pq)^{0.292}$ криптосистема стає нестійкою. Ще пізніше у 2004 році Дж. Блоумер та О. Мей узагальнили атаку Вінера, використовуючи розкладання числа у неперервний дріб та алгоритм редукції на решітках. Автори показали, що для кожного відкритого ключа (n,e) якщо виконується: $ex + y \equiv 0 \pmod{\phi(n)}$, для деяких $x < \frac{1}{3}n^{-\frac{3}{4}}$ та $|y| \leqslant excn^{-\frac{3}{4}}$, c - константа, тоді знайти числа p та q можна за поліноміальний час [8].

Роком раніше Дж. Блоумер та О. Мей опублікували роботу [9], у якій була описана атака на криптосистему RSA, яка використовує метод Копперсміта. А саме, у 1997 році Д. Копперсміт [10] описав ефективний алгоритм знаходження розв'язку рівнянь виду $a_k x^k + \cdots + a_1 x + a_0 \equiv 0 \pmod{M}$, де модуль M та коефіцієнти полінома є цілими числами. А також метод для знаходження коренів аналогічного поліноміального рівняння, але з двома змінними. Було показано, як знаючи певну кількість значущих бітів секретної експоненти d факторизувати модуль криптосистеми RSA, за умови що відкрита експонента обмежена деякими значеннями. Тобто, якщо $n^{\frac{1}{2}} \leqslant e \leqslant n^{0.725}$, то знаючи α найстарших значущих біт ($Most\ significant\ bits$, далі

$MSBs$) числа d, відкритий ключ n можна факторизувати за час $O((log_2 n)^c)$, де c деяка константа. Значення α залежить від розміру відкритої експоненти, зі збільшенням розміру e збільшується кількість необхідних значущих біт. Так само було доведено, що модуль RSA можна факторизувати за поліноміальний час знаючи хоча б половину $MSBs$ числа $d_p = d \pmod{(p-1)}$, за умови що відкрита експонента $e < n^{0.25}$. Аналогічно була побудованна атака, яка базується на відомих наймолодших значущих бітах ($Least\ significant\ bits$, далі $LSBs$) секретної експоненти, і застосовна до криптосистеми RSA у якій відкритий ключ e менший за $n^{0.875}$. Також у 2004 році А. Дуджелла узагальнив результат Лежандра про наближення дійсного числа раціональним нескоротним дробом [11]. Це дало можливість покращити вищезгадані атаки на криптосистему з невеликим секретним ключем d.

У 2009 році Н. Хенінгер та Х. Шахам запропонували ефективний алгоритм відновлення секретних ключів криптосистеми RSA, якщо відома деяка кількість їх бітів. Особливість запропонованої атаки, полягає у тому, що відомі біти не повинні бути найстаршими або наймолодшими, а також йти послідовно, важлива тільки їх кількість та значення. Алгоритм ефективно відновлює секретні ключі у таких випадках [12]:

1) Коли відомо 27% біт кожного з секретних ключів: p, q, d, $d \pmod{p}$ та $d \pmod{q}$.

2) Коли відомо 42% біт кожного з секретних ключів: p, q та d.

3) Коли відомо 57% біт кожного з простих чисел p та q.

Однак, треба зазначити, що дана атака є імовірнісною і зі збільшенням довжини секретних параметрів імовірність успіху зростає. Також вона має поліноміальну часову складність.

Якщо правильно обрані параметри криптосистеми, то стійкість RSA залежить від складності задачі факторизації та складності задачі дискретного логарифмування. На зараз найефективніший алгоритм факторизації має субекспоненційну складність. Відповідно до [13] для натуральних чисел $n < 10^{110}$ найефективнішим алгоритмом факторизації

є алгоритм квадратичного решета з використанням декількох многочленів. Для натуральних чисел $n > 10^{110}$ найефективнішим є алгоритм решета числового поля, який описано у [14]. Складність за часом цього алгоритму оцінюється як $L_n[1/3, \sqrt[3]{(64/9)}]$ [30]. У серпні 2010 року група вчених з Швейцарії, Японії, Германії, Франції, США та Нідерландів факторизували число довжиною 768 бітів за допомогою методу решета числового поля [15]. Тому задля збереження стійкості краще використовувати відкритий ключ n довжини не менше 1024 бітів.

1.2 Модифікації криптосистеми RSA

Після запропонування односторонньої функції RSA почали з'являтись інші криптосистеми, які також використовують арифметику за модулем. Зокрема, Рівест, Шамір та Адлеман у своєму патенті 1977 року [16] зауважили, що можливо використовувати модуль $n = p_1^{k_1} p_2^{k_2} \dots p_l^{k_l}$. Тому протягом наступних років було побудовано багато модифікацій криптосистеми RSA.

Спочатку у 1982 році Дж.-Дж. Квісквотер та К. Коуврер запропонували новий спосіб розшифрування у криптосистемі RSA [17] (далі метод Квісквотера-Коуврера). У цьому методі використовується наслідок з Китайської теореми про лишки (далі КТЛ) та теоретично він приблизно в 4 рази швидше ніж алгоритм розшифрування у RSA [18]. Пришвидшення відбувається за рахунок того, що секретну експоненту d беруть за модулем $p - 1$ та за модулем $q - 1$, і для розшифрування вже використовуються лишки, які суттєво менші за значення d. Отже, метод Квісквотера-Коуврера дозволяє збільшити швидкість розшифрування і при цьому використовувати секретний ключ d достатньо великої довжини для забезпечення стійкості.

У 1991 році К. Кояма, Ю.М. Моркер, Т. Окамото та С.А. Ванстоун першими запропонували аналог криптосистеми RSA (далі $KMOV$) на еліптичних кривих над кільцем Z_n [19]. Зокрема, у їх роботі описано три

нові класи односторонніх функцій, кожен з яких використовується для різних задач. Перший не може використовуватися для криптосистеми з відкритим ключем, а тільки для цифрового підпису (далі ЦП). Другий та третій класи вже є аналогом криптосистем: RSA та Рабіна [20], у них використовується модуль $n = pq$, де прості числа : $p \equiv q \equiv 2 \pmod 3$. Стійкість запропонованих криптосистем на еліптичних кривих також ґрунтується на складності факторизації числа n. Незважаючи на те, що криптосистема $KMOV$ повільніша за класичну RSA, у [19] зазначалося, що вона має бути стійкою до атак з невеликим відкритим ключем e. Але, автори роботи [21] показали, що ця криптосистема вразлива до атак з невеликою шифрувальною експонентою. Потім у 1993 році Н. Демитко [22] запропонував інший аналог криптосистеми RSA на еліптичних кривих над кільцем Z_n, покращення криптосистеми $KMOV$. Повідомлення у криптосистемі Демитко це перша координата точки $M(x,y)$, яка належить кривій $y^2 \equiv (x^3 + ax + b) \pmod n$. Зашифрування відбувається шляхом e-кратного додавання точки M: $C = eM = (x_c,y_c)$, а шифротекст визначається як перша координата точки C. Експонента d для розшифрування обирається в залежності від символів Лежандра $(\frac{z}{p})$ та $(\frac{z}{q})$, де $z \equiv (x_c^3 + ax_c + b) \pmod n$. Також для пришвидшення розшифрування можна застосовувати КТЛ. Ще пізніше у 1995 році К. Кояма описав криптосистему побудовану на сингулярній еліптичній кривій, розшифрування в якій у 2 рази швидше за розшифрування в класичній RSA для повідомлень довжиною $2log_2(n)$ [23]. Треба зазначити, що у криптосистемі $KMOV$ додавання точок еліптичної кривої за складеним модулем, задається так само, як і додавання точок еліптичної кривої над полем. Тому у кільці Z_n додавання не завжди визначено, однак для великих простих чисел p та q ймовірність отримати невизначену суму несуттєва.

Також одним з ключових параметрів у криптосистемі RSA є вибір довжини відкритого ключа n, адже це безпосередньо впливає на її швидкість та стійкість. Треба враховувати, що занадто великий модуль

дуже сповільнить функціонування системи, у той час як до занадто малого відкритого ключа застосовні алгоритмі факторизації. Тому при виборі розміру параметрів завжди треба жертвувати одним на користь іншого. Однак, у 1995 році А. Шамір опублікував статтю "RSA для параноїків-[25], у якій запропонував оптимальне рішення для збереження стійкості криптосистеми без втрати часу. Автор назвав цю систему незбалансована RSA (далі $Unbalanced\ RSA$). У цій криптосистемі довжина модуля n 5000 біт, у той час як розмір простих чисел p та q: 500 та 4500 бітів відповідно.

У 1997 році Т. Такагі запропонував N-адичне розширення криптосистеми RSA [26]. У якості модуля обирається число $n^k = (pq)^k$, де p та q різні прості, а число k залежить від розміру повідомлення. А саме k - це кількість блоків, на які розбивається повідомлення $M : M_0, \ldots, M_{k-1}$, де всі $M_i < n$, i від 0 до $k-1$. Відкритий ключ e та секретний ключ d задовольняють співвідношенню $ed \equiv 1 \pmod{\text{НСК}(p-1, q-1)}$. Розшифрування першого блоку відбувається за такий самий час як і в криптосистемі RSA. А для інших блоків складаються лінійні рівняння, кількість яких залежить від числа k. Цей процес, так само як і процес розв'язування лінійних рівнянь, вимагає стільки ж часу, скільки і шифрування в N-адичному розширенні криптосистеми RSA.

Твердження 1.1. *[26] Для описаного N-адичного розширення криптосистеми RSA справедливо: Якщо на множині відкритих текстів $\mathbb{M}$ заданий рівноімовірний розподіл, то знайти відкритий текст за відомим шифротекстом так само складно як і в криптосистемі RSA.*

Також у 1997 році Т. Коллінз, Д. Хопкінс, С. Лангфорд та М. Сабін [27] запатентували ефективний метод використання RSA зі складеним модулем (далі $MF - RSA$). У цій криптосистемі використовується відкритий ключ $n = p_1 p_2 \ldots p_l$, де $l \geqslant 3$. Шифрування відбувається як і в класичній RSA, а розшифрування відбувається частинами, завдяки використанню методу Квісквотера-Коуврера.

Переваги цієї криптосистеми у тому, що можна використовувати прості числа меншої довжини без втрати стійкості. Однак треба зазначити, що секретні параметри слід обирати так, щоб алгоритм факторизації за допомогою еліптичних кривих (далі метод Ленстри) [28] був незастосовним. Якщо, наприклад, $l = 3$ тоді для відкритого ключа довжиною 1024 біти $MF - RSA$ приблизно в $\frac{9}{4}$ разів швидше за класичну RSA [29]. Отже, у $MF - RSA$ збільшується кількість секретних параметрів, у той час як їх розмір зменшується. Це дозволяє дещо спростити етап створення ключів.

У 1998 році Т. Такагі запропонував модифікацію криптосистеми RSA [30], яка використовує модуль $n = p^k q$. Її будемо називати $PP - RSA$ (Prime Power RSA). Секретні параметри криптосистеми p та q обираються так, щоб алгоритми факторизації решета числового поля або метод Ленстри не можна було б застосувати до числа n. Відкритий та секретний ключі e та d є взаємообернені за модулем НСК($p-1$,$q-1$). Шифрується повідомлення так само як і в криптосистемі RSA. А ось розшифрування відбувається частинами, тобто окремо обчислюється частина повідомлення за модулем p^k та q, а потім застосовується наслідок з КТЛ. Зокрема для розшифрування частини повідомлення за модулем p^k використовується алгоритм запропонований Такагі для N-адичного розширення криптосистеми RSA. Для випадку коли $k = 2$, а довжина p та q по 256 біт, $PP - RSA$ приблизно в півтора рази швидше за криптосистему RSA [30].

Потім у 2000 році С. Лім, С. Кім, І. Йие та Х. Ліі узагальнили криптосистему $PP - RSA$, запропонувавши використовувати модуль $n = p^k q^l$. Назвемо узагальнену криптосистему $GPP - RSA$ (*Generalized Prime Power RSA*). Всі параметри $GPP - RSA$ задовольняють тим же вимогам, що і криптосистема $PP - RSA$, а також шифрування та розшифрування відбувається за запропонованими алгоритмами Т. Такагі. Було більш точно обчислено складність роботи алгоритму розшифрування за модулем вигляду m^r. Зокрема, у

криптосистемі $GPP - RSA$ для відкритого ключа $n = p^k q^l$ складність розшифрування, за умови, що прості числа p та q мають однакову бітову довжину дорівнює: $L = (log_2 p)^3 + (\frac{k(k+1)(2k+1)+l(l+1)(2l+1)}{6}) \cdot (log_2 p)^2$ [31]. Коли числа k та l приблизно однакові за значенням, то величина L набуває мінімального значення, вважаючи, що $k + l$ фіксоване число. Для забезпечення стійкості криптосистеми $GPP - RSA$ необхідно, щоб НСД(k,l) $= g = 1$, оскільки складність розкладання на множники числа $n = p^k q^l$ еквівалентна складності факторизації числа $n' = p^{\frac{k}{g}} q^{\frac{l}{g}}$.

Твердження 1.2. *[31] Для RSA-подібних криптосистем з модулем виду: $N = p_1^{k_1} p_2^{k_2} \dots p_l^{k_l}$, найбільш швидке розшифрування досягається коли $l = 2$, k_1 та k_2 приблизно однакові за значенням, та за умови, що не використовується паралельне обчислення.*

У роботі 2002 року Д. Боне та Х. Шахам [29] проаналізували декілька варіантів раніше запропонованих систем типу RSA: $Batch\ RSA$, $MF - RSA$ разом з $PP - RSA$, та $RebalancedRSA$. Детально було описано функціонування криптосистеми $RebalancedRSA$, яка ґрунтується на пропозиції Вінера [32]. Головна ідея - це спробувати зробити розшифрування та створення ЦП ефективнішим та швидшим ніж шифрування та перевірка ЦП. У цій криптосистемі пропонується зменшити час розшифрування за рахунок значного збільшення відкритої експоненти. Досягається це шляхом випадкового вибору секретного ключа d, який задовольняє наступним рівностям: $d = r_p \pmod{(p-1)}$ та $d = r_q \pmod{(q-1)}$, де r_p та r_q - випадкові числа, довжина яких l і вони не перевищують $\frac{pq}{2}$. При цьому розмір d достатньо великий для забезпечення стійкості. У криптосистемі $RebalancedRSA$ розшифрування відбувається швидше ніж у RSA приблизно в $\frac{n}{2l}$, за умови що p та q однакової довжини [29]. Відповідно, для 2048-бітного модуля та для $l = 160$ біт розшифрування пришвидшується в 6,4 рази.

Потім у 2003 році С. Е. М. Пейшао описав криптосистему $RPrime\ RSA$ [33], яка є поєднанням криптосистем: $MF - RSA$ та

$RebalancedRSA$. Зокрема, створення ключів відбувається аналогічно у $RebalancedRSA$, тільки замість двох простих чисел, отримують r простих чисел. Параметр l відповідає довжині випадкових чисел. Шифрування повідомлення нічим не відрізняться від шифрування у криптосистемі RSA. А ось розшифрування відбувається за алгоритмом $MF - RSA$. Тому, теоретично, пришвидшення в $RPrime\ RSA$ дорівнює $\frac{log_2(n)r}{4l}$, і для розміру модуля 2048 біт розшифрування відбувається в 27 разів швидше ніж в криптосистемі RSA та в 8 разів швидше за метод Квісквотера-Коуврера [33]. Слід зауважити, що в $RPrime\ RSA$ пришвидшення розшифрування залежить від кількості простих чисел у відкритому ключі, а також від їх розміру.

У 2018 році М. Будабра та А. Нітай узагальнили криптосистему $KMOV$ (далі $GKMOV$), використовуючи еліптичну криву $y^2 \equiv (x^3 + b) \pmod n$, де модуль $n = p^k q^l$ [34]. Прості числа у данній криптосистемі мають вид $3k + 2$, як і в $KMOV$, а число b задовольняє умові: НСД(b,pq) = 1. Проаналізовано стійкість нової криптосистеми до різного типу атак. Система $GKMOV$ є стійкою до таких атак: знаходження простого дільника числа n, знаходження порядку еліптичної кривої, знаходження відкритого тексту за відомим шифротекстом, знаходження секретної експоненти d (якщо d не занадто маленьке). Так само, як і в $KMOV$ додавання точок еліптичної кривої над кільцем $Z_{p^k q^l}$ визначено не завжди, а саме в тих випадках коли не існує оберненого елементу за модулем p^k або q^l. Доведено, що ймовірність того, що сума двох точок раніше вказаної еліптичної кривої виявиться невизначеною дорівнює приблизно: $\frac{p+q}{(p+1)(q+1)}$ [34].

1.3 Наявні атаки на різні модифікації криптосистеми RSA

З появою нових криптосистем типу RSA, їх починають більш детально досліджувати на аналізувати на вразливість до вже наявних атак. Зокрема, дуже багато атак на вищеописані криптосистеми

побудовані як розширення атак на криптосистему RSA. Далі коротко будуть наведені деякі результати з криптоаналізу криптосистем: $KMOV$, $PP-RSA$, $GPP-RSA$ та $MF-RSA$.

Розглянемо відомі атаки на криптосистему $KMOV$ та її покращення, яке описав Н. Демитко [22]. У 1995 році Р. Пінч у [35] розширив атаку Вінера з малою секретною експонентою на криптосистему типу RSA на еліптичних кривих. Зокрема, для криптосистеми $KMOV$ секретний ключ d має бути не менше за $n^{\frac{1}{4}}$, а для покращення Демитка не менше ніж $n^{\frac{1}{8}}$. У 1997 році С. Каліський [36] показав, що ця криптосистема вразлива до атак на основі обраного відкритого тексту або шифротексту. Також до неї застосовна атака з малою відкритою експонентою. Потім у 1999 році С. К. Чуа, К. Х. Леунг та С. Лінг [37] описали атаку на криптосистему описану у роботі [24]. Якщо два відкритих тексти пов'язані між собою лінійним перетворенням, то криптоаналітик зможе знайти один з них. У статті описується ділення поліномів на кубічних еліптичних кривих, яке потім використовується для побудови атаки. Ще було показано, що криптосистема К. Коями [23] зводиться до криптосистеми криптосистеми з публікації [24]. Отже, описана атака є застосовною до обох криптосистем. У 2008 році було опубліковано роботу Б. Ібрагімпашича, у якій розширено атаку [11] на криптосистему $KMOV$. Зазначено, що відкритий ключ n криптосистеми $KMOV$, довжина якого 1024 біти, можна факторизувати за поліноміальний час, якщо довжина секретної експоненти d менше 270 біт [38]. Ще одна атака на $KMOV$ була побудована у роботі А. Нітаджа:

Твердження 1.3. *[39] Нехай $n = pq$, де $q < p < 2q$ відкритий ключ криптосистеми $KMOV$. Нехай публічна експонента e задовольняє рівності: $ex - (p+1)(q+1)y = z$, при умові що: НСД$(x,y) = 1$, $xy < \frac{\sqrt{2n}}{12}$ та $|z| < \frac{(p-q)yn^{\frac{1}{4}}}{3(p+q)}$, тоді число n можна факторизувати за поліноміальний час.*

У доведенні твердження, подібно до атак на криптосистему RSA,

також використовується алгоритм редукції на решітках та наближення дійсного числа раціональними дробами.

Дуже багато атак було побудовано на криптосистему $PP-RSA$. У більшості з них автори використовували той факт, шо секретний ключ d є оберненим до e за модулем $\phi(n)$, хоча у роботі Т. Такагі зазначалося, що відкрита та секретна експоненти повинні задовольняти співвідношенню: $ed \equiv 1 \pmod{\text{НСК}(p-1,q-1)}$. Спочатку у 1999 році Д. Боне, Г. Дерфи та Н. Хаугрейв-Грэм побудували атаку на криптосистему $PP-RSA$ використовуючи цілочисельні решітки. Атака полягає в тому: якщо степінь k для модуля $n = p^k q$ занадто великий, то число n можна факторизувати за час поліноміальний час. Час роботи запропонованого алгоритму факторизації дорівнює: $T(r) = 2^{r^{(1-\epsilon)}+O(log_2 r)}$, де степінь $k = r^{\epsilon}$, а r це бітова довжина простих чисел p та q [40]. Видно, що занадто великий степінь, це коли k дорівнює r або більше за нього. У цьому випадку час роботи алгоритму займає $O(k^c)$, де c - фіксована константа. Також запропонований алгоритм детермінований і має поліноміальну просторову складність.

У 2004 році А. Мей запропонував декілька атак на модифікацію криптосистеми RSA з модулем $n = p^k q$ [41], які направлені на знаходження секретної експоненти d. Результат Копперсміта [10] для рівнянь з однією змінною використав Мей для побудови таких атак. Доведено два головних результати, а саме: знаючи $1 - \frac{k}{(k+1)^2}$ найстарших або наймолодших значущих біт числа d можна факторизувати відкритий ключ n за поліноміальний час. Формулювання другого твердження аналогічне, але тут оцінка сягає до $\frac{4k}{(k+1)^2}$ значущих біт секретної експоненти. Також було узагальнено атаку [9] для системи $PP-RSA$, яка потребує $\frac{1}{k+1}$ значущих (найстарших або наймолодших) біт числа $d_p = d \pmod{(p-1)}$ для знаходження простого дільника модуля n.

У 2008 році К. Ітo, Н. Кунігіро та К. Куросава у своїй роботі [42] описали, ще одну атаку на криптосистему Такагі. Доведено, що секретну експоненту можна знайти за поліноміальний час, якщо вона є меншою за

значення $n^{\frac{2-\sqrt{2}}{k+1}}$. Важливим є той факт, що ключі e та d обернені за модулем $(p-1)(q-1)$. Також, запропонована атака є узагальненням атаки [7]. Зокрема, для її побудови використовується метод пошуку коренів полінома від трьох змінних за модулем e та алгоритм редукції базису решітки. Також у 2014 році С. Саркар у своїй роботі [43] покращив результат [41], для значення степені $k \leqslant 5$. Зокрема, для випадку коли $k = 2$, модуль криптосистеми $PP - RSA$ можна факторизувати за поліноміальний час, якщо $d \leqslant n^{0.395}$. Для цього автор використовував метод, який ґрунтується на алгоритмі знаходження базису цілочисельної решітки [45]. Потім, у 2016 році опубліковано ще одну роботу Саркара [44], у якій покращено попередню оцінку для значень степенів $k = 3$ та $k = 4$. Варто зазначити, що на відміну від роботи Ітo, Кунігіро та Куросави, атака була побудована для криптосистеми, у якої відкрита та секретна експоненти пов'язанні співвідношенням: $ed \equiv 1 \pmod{\phi(n)}$, так само як і в роботі [41]. У 2014 році Яо Лу, Р. Чжан, Л. Пен і Д. Лінь у своїй роботі [47] запропонували новий метод пошуку коренів рівняння $p(x_1,\ldots,x_l) \equiv 0 \pmod{q^d}$, де q^d невідомий дільник деякого цілого числа M, а $p(x_1,\ldots,x_l)$ - поліном від декількох змінних з цілочисельними коефіцієнтами. Їхні оцінки верхньої межі секретної експоненти виявилися кращими ніж оцінки [41] та [44] для степені $k > 4$.

У 2015 році А. Нітай та Т. Рачіді [46] побудували 3 атаки на криптосистему $PP - RSA$. Перша атака можлива, за умови, що відкритий ключ e задовольняє нерівність $ea - \phi(n)b = c$ для деяких цілих невід'ємних чисел a та c, та цілого числа b. Наведена нерівність є узагальненим випадком нерівності в роботі [43], де значення c дорівнювало 1. Показано, що для швидкої факторизації числа n необхідно, щоб $|ac| < n^{\frac{k(k-1)}{(k+1)^2}}$. Друга атака використовує співвідношення між двома секретними експонентами, а саме, якщо модуль їх різниці $\Delta < n^{\frac{k(k-1)}{(k+1)^2}}$, то знайти нетривіальний простий дільник модуля $PP - RSA$ можна за поліноміальний час. Третя атака також використовує близькість значень секретних параметрів. Якщо два відкритий ключа

$n_1 = p_1^k q_1$ та $n_2 = p_2^k q_2$ криптосистеми $PP - RSA$ створено так, що різниця чисел p_1 та p_2 не перевищує значення $\frac{p_1}{2kq_1q_2}$, то можна ефективно знайти секретні ключі. Перші дві атаки ґрунтуються на одній й тій самій теоремі про ефективне знаходження коренів полінома за складеним модулем, які сформульовано в роботі [47]. Третя атака використовує відомий результат Лежандра про наближення числа нескоротним дробом. У цьому ж році було побудовано ще одне узагальнення атаки Саркара, у роботі [48].

Також у роботі [49] О. Акшишч та О. Хадір запропонували ще один ефективний спосіб знаходження простих дільників модуля криптосистеми $PP - RSA$. На застосування атаки витрачається час, обмежений деяким поліномом від $log_2(n)$. Побудований алгоритм факторизації, який повертає прості дільники числа n, якщо секретна експонента достатньо близька за значенням до числа виду lp^r, де l та $0 < r < k$ цілі числа (знати які не обов'язково).

У 2019 році С. Шеху та М. Р. К. Аріфін у [50] описали, ще три атаки на модифікацію криптосистеми RSA модулем $n = p^k q$. Перша атака для розкладання модуля криптосистеми використовує розкладання числа у неперервний дріб, і вимагає, щоб відкрита експонента задовольняла умову:

$$ex - ny + (q^k + p^k u)y = z \tag{1.1}$$

Також показано, що кількість відкритих ключів e, які задовольняють співвідношення (1.1) не менше ніж $n^{\frac{5k-7}{6(k+1)}-\varepsilon}$. Дві інші атаки використовують l різних модулів криптосистеми $PP - RSA$ однакової довжини та з однаковим степенем k. Зокрема, для другої атаки всі l відкритих експонент повинні задовольняти умову (1.1), для різних параметрів, але з однаковими значеннями x та u. Третя атака також вимагає виконання умови (1.1) для l різних відкритих ключів e_j, проте тут вже параметри y та u однакові у всіх рівностях. Атаки дозволяють

факторизувати всі l модулів $PP-RSA$ за поліноміальний час. Для часткового випадку $PP-RSA$ з параметром $k=2$ у 2015 році М. Асболлою та М. Аріффіном запропонована атака з використанням наближених дробів. Автори використовують близькість значень простих чисел p та q: якщо $2p^{\frac{5}{3}}|p^{\frac{1}{3}}-q^{\frac{1}{3}}|<\frac{1}{3}n^{\alpha}$, та секретна експонента обмежена $d<n^{\frac{1-\alpha}{2}}$ [51] - то це призведе до зламу криптосистеми з модулем p^2q. Зовсім нещодавно у лютому 2021 року опублікована ще одна робота [60], у якій побудована ще одна атака на криптосистему з модулем p^2q. Вона також належить до класу атак з частковим знанням секретного ключа, і застосовна якщо створено хоча б дві пари відкритих та секретних експонент за одним і тим самим модулем. Якщо секретні ключі p та q мають певну кількість спільних наймолодших значущих біт, а значення $|d_1-d_2|$ не перевищує n^{α}, то модуль криптосистеми можна факторизувати за поліноміальний час.

Далі розглянемо атаки, які були побудовані на криптосистему $GPP-RSA$. У 2015 році Я. Лу, Л. Пен і С. Саркар запропонували різни атаки на дану криптосистему. Вони використовували конструкцію побудовану на цілочисельних решітках, та ефективний метод знаходження коренів модульного поліноміального рівняння, який базується на роботі Коперсміта. Атаки дозволять факторизувати модуль $n=p^kq^l$, якщо відома $\min\left(\frac{l}{l+k},\frac{2(k-l)}{l+k}\right)$ кількість найстарших або наймолодших значущих біт секретного ключа p. Також була розширена атака з малою серктеною еспонентою d для криптосистеми $GPP-RSA$. Важливо, що результати були наведені для двох варіантів створення пари експонент e та d. Коли виконується конгруенція $ed\equiv 1 \pmod{\phi(n)}$, для того щоб знайти секретну експоненту, необхідно : $d<N^{1-\frac{3k+l}{(r+l)^2}}$ [52]. Для варіанту коли пара експонент обернені за модулем $(p-1)(q-1)$ та якщо виконується умова $d<N^{\frac{1}{2(r+l)}}$ [52], тоді можна знайти секретні ключі p та q за поліноміальний час.

У 2016 році Дж.-С. Корон, Дж.-Ч. Фужеар, Г. Рено, Р. Зейтун розширили атаку 1999 року, яка була побудована на криптосистему

$PP-RSA$ та застосовна у тому випадку, коли степінь k занадто довга. Розглядається випадок, коли ступені k та l більше за значення $(loq_2p)^3$, що призводить до факторизації модуля за поліноміальний час [53]. Використаний той факт, що степені k та l можна подати у вигляді: $k = Na + c,\ l = Nb + d$, де достатньо N велике додатне число, та a, b, c, d - невеликі додатні числа. З цього випливає, що модуль криптосистеми має вигляд $n = p^{Na+c}q^{Nb+d} = (p^aq^b)^Np^cq^d = X^NY$, що дає можливість застосовувати алгоритм факторизації [40] для знаходження чисел X та Y, а потім вже простих дільників p та q.

Потім у 2018 році М. Зенг запропонував новий метод факторизації модуля криптосистеми $GPP-RSA$ на основі цілочисельних решіток. Було побудовано декілька атак з використанням «цілочисельного методу» — метод знаходження коренів цілочисельного поліноміального рівняння. Для того, щоб знайти не тривіальні прості дільники числа $n = p^kq^l$, необхідно знати $n^{\frac{1}{l+k}-\gamma}$ найстарших значущих бітів секретного ключа p (або q), де кількість невідомих біт параметрів p та q обмежене числом n^γ [54]. Показано, як знаючи α_p найстарших значущих бітів числа p, знайти таке наближення α_q для простого числа q, щоб виконувалась нерівність: $|q - \alpha_q| < n^\gamma$. Накращі (тобто наймешна кількість значущих біт необхідна) оцінки були отримані для параметрів: $k = 3$, $l = 2$ та $k = 5$, $l = 3$. У цих двох випадках цілочисельний метод більш ефективний ніж атаки, які ґрунтуються на методі розв'язування модульних поліноміальних рівнянь.

У 2002 році М. Сиет, Ф. Коун, Ф. Лагиллоуми та Дж.-Дж. Квісквотер розширили атаки [7] та [32] для криптосистеми $MF-RSA$. Модуль цієї криптосистеми має вигляд $n = p_1p_2 \cdot \ldots \cdot p_l$, де все l простих чисел різні. Атака з використанням наближених дробів, яку запропонував М. Вінер для криптосистеми RSA здійсненна, якщо секретна експонента d приблизно менше ніж $n^{\frac{1}{2l}}$ [55]. Друга атака використовує техніку, яка базується на цілочисельних решітках та базується на емпіричному методі. Автори не рекомендують

використовувати секретну експоненту розмір якої є менше ніж n^{γ}, де $\gamma = \frac{4}{3} - \frac{1}{3l} - \frac{2}{3l}\sqrt{4l^2 - 5l + 1}$ [55]. Автори показали, що використання невеликої секретної експоненти іноді недоцільно, адже є методи які достатньо ефективно зламують криптосистему $MF - RSA$ в деяких випадках, наприклад коли $l = 3$. Однак, ці дві запропоновані атаки втрачають свою ефективність зі збільшенням кількості простих чисел у модулі $n = p_1 p_2 \cdot \ldots \cdot p_l$.

Далі у 2003 році М. Дж. Хінек, М. К. Лоу та Е. Теске розглядали атаки на криптосистему RSA та їх можливе розширення на криптосистему $MF - RSA$. Показано, що використання публічної експоненти $e = 3$ дає можливість зловмиснику знайти $\frac{1}{l}$ частину секретної експоненти d. Розглянуті розширення атак: з частковим знанням секретного ключа, з невеликою секретною експонентою, з невеликою відкритою експонентою. Для побудови використовувались алгоритми, які базуються на цілочисельних решітках та наближення нескоротними дробами. Було показано, що розширення метода [7] коли $l \geqslant 3$ можливе, але працювати він буде не ефективно. Доведено, що якщо відомо $n - k$ біт секретного ключа d, то його можна відновити за час $O(\frac{n^3 l}{\varepsilon})$, де значення k задовольняє нерівності $2^k < e < 2^{k+1}$, а $0 < \varepsilon < 1$ [56]. У роботі [57] 2008 року були зібрані всі наявні на той час атаки на $MF - RSA$. Показано, що атаки які спрямовані на знаходження секретних ключів $p_1, p_2, \ldots, p_l$ з використанням тільки числа n не залежать від значення l. Тобто кількість простих чисел у модулі не впливає на складність факторизації, а залежить тільки від бітового розміру значення n. Так само, для $MF - RSA$, яка використовує метод Квісквотера-Коуврера для пришвидшення шифрування, на ефективність побудованої атаки не впливає вигляд модуля, тобто складність залежить тільки від його довжини та відкритої експоненти e. Однак, деяка залежність від значення l все ж таки присутня, тому що для знаходження всіх простих чисел модуля, необхідно застосувати алгоритм факторизації $l - 1$ раз. Для практичної реалізації зазвичай використовують значення $l = 3, 4, 5$, тому

ця залежність вважається несуттєвою. Атаки, які використовують відомі найстарші або наймолодші значущі біти секретних параметрів стають складнішими зі збільшенням кількості простих чисел. Також атаки на криптосистему $MF-RSA$ з невеликою секретною експонентою стають неефективними зі зростанням кількості простих множників модуля. У 2013 році Х. Занг і Т. Такагі побудували дві нові атаки на криптосистему $MF-RSA$, які застосовні, якщо прості дільники модуля є близькими за значенням. Недивлячись на те, що атаки з малою секретною експонентою на $MF-RSA$ є неефективними, як зазначалося у [57], у випадку невеликої різниці між секретними параметрами побудований швидкий алгоритм. Автори показали, що використання малої секретної експоненти d може бути небезпечним. Перша атака є імовірнісною, та описує як знайти секретну експоненту d за час $O(log_2 n)$, якщо виконуються наступні умови: $p_1 < p_2 < \ldots < p_l$ - прості числа однакової довжини, $p_l - p_1 = n^{\alpha}$, де $0 < \alpha < \frac{1}{l}$ та $d = n^{\varepsilon}$, де $\varepsilon < 1 - \sqrt{1 + \alpha - \frac{2}{l}}$ [58]. Друга атака дозволяє факторизувати модуль за час $O(log_2 n)$, за тих же умов на прості числа p_1,p_2,...,p_l, тільки показник $\alpha > 0$ повинен бути не більше ніж $\frac{1}{l^2}$. Отже, якщо у $MF-RSA$ обирається невелика секретна експонентна d, доречно буде перевіряти різницю між простими числами криптосистеми задля уникнення запропонованої атаки.

Потім М. Зенг, Н. Кунігіро та Х. Ху в 2017 році запропонували дві покращені атаки на криптосистему $MF-RSA$, які використовують близькість простих чисел. Побудова атак, використовує ті самі ж методи, що й атака [58]. Автори пропонують замість l різних лінійних модульних рівнянь, як було зроблено у роботі Занга та Такагі, розв'язувати одне лінійне рівняння багатьох змінних використовуючи цілочисельні решітки. Так само вважається, що прості числа впорядковані та $p_l - p_1 = n^{\alpha}$, і у випадку коли $l = 3$, необхідно, щоб $\alpha < \frac{2}{l(l+2)}$ [59] для вдалої факторизації модуля n за поліноміальний час. Коли значення $l > 3$, то вимагається, щоб $\alpha < \frac{2}{l(r+1)} \left(\frac{1}{l}\right)^{\frac{1}{r}}$, для деякого параметра r, який знаходиться в залежності від кількості простих чисел у модулі.

Висновки до розділу 1

У розділі розглянута криптосистема RSA та різні атаки на цю криптосистему. Враховуючи те, що одними з головних параметрів криптосистеми є довжина модуля, а також швидкість розшифрування, почали з'являтися альтернативні варіанти криптосистем які використовують ідею RSA. Запропоновані модифікації загалом побудовані задля:

1) зменшення часу розшифрування;

2) пришвидшення етапу створення ключів (випадкових простих чисел заданої довжини);

3) забезпечення стійкості до існуючих атак на RSA.

Нові криптосистеми, як $PP - RSA$ та $GPP - RSA$, виявились вразливими до багатьох вже наявних атак на RSA з деякими розширеннями. Серед них атаки: з частковим знанням секретного ключа, з малою відкритою експонентною та з малою секретною експонентною. Однак, також доведено, що для $MF - RSA$ перші два типи атак стають неефективними зі зростанням кількості простих чисел у модулі. Атаки з частковим знанням секретного ключа для криптосистем RSA, $PP - RSA$ та $GPP - RSA$ потребують значну кількість найстарших або наймолодших значущих біт секретних параметрів криптосистем. Наприклад, для криптосистеми RSA для здійснення імовірнісної атаки факторизації необхідно більше половини наймолодших значущих біт простих чисел. Для випадку $PP - RSA$ атаки або використовую значущі біти секретною експоненти, або вимагають, щоб прості числа мали деякі спільні найстарші значущі біти. Аналогічно і для криптосистеми $GPP - RSA$, більшість атак побудована на використанні значущих біт секретної експоненти. Однак також побудована атака, яка потребує найстарші значущі біти простого дільника модуля криптосистеми $GPP - RSA$.

Отже, атаки з частковим знанням секретного ключа, які використовують наймолодші значущі біти для модифікацій криптосистеми досліджені не дуже досконало, у той час як для класичної RSA побудовано декілька таких атак. Більш того, для криптосистеми RSA вони вимагають значну кількість бітів секретних ключів. Доречно буде розглянути розширення атаки з частковим знанням секретного ключа на модифікації криптосистеми RSA.

2 ПОБУДОВА АТАКИ НА КРИПТОСИСТЕМУ RSA ТА ЇЇ МОДИФІКАЦІЇ

У цьому розділі розглянуто атаку на криптосистему RSA, у якій прості числа задовольняють спеціальному виду. Робиться покращення цієї атаки за умови, що є відома деяка кількість наймолодших значущих бітів секретних ключів. Більш детально розглядається криптосистеми Т. Такагі $PP - RSA$, а також її узагальнення $GPP - RSA$. Описується як побудувати розширення атаки з відомими наймолодшими значущими бітами на криптосистеми $PP - RSA$ та $GPP - RSA$. На прості числа модифікацій RSA також накладаються додаткові умові, тому також було оцінено кількість простих чисел, які задовольняють ці вимоги.

2.1 Покращення атаки на криптосистему RSA

Розглянемо криптосистему RSA, яка будується таким чином:

1. **Етап створення ключів:**

1) Випадковим чином обираємо p та $q \in \mathbb{Z}_+$ - різні прості числа приблизно однакової довжини;

2) Обчислюємо $n = pq$ та $\phi(n) = (p-1)(q-1)$;

3) Обираємо таке число e, що $1 < e < \phi(n)$ та НСД$(e, \phi(n)) = 1$;

4) Обчислюємо число $d = e^{-1} \pmod{\phi(n)}$ - обернене до e за модулем числа $\phi(n)$.

Маємо (e,n) - відкритий ключ та $(p, q, \phi(n), d)$ - секретний ключ.

2. **Шифрування:** Вважаємо, що відкритий текст $M \in \mathbb{Z}_n$ та $M > 1$

1) $M^e \pmod{n} = C$ - шифротекст.

3. **Розшифрування:**

1) $C^d \pmod{n} = M$ - відкритий текст.

У роботі 2020 року А. Гафар, М. Аріффін та М. Асболла

побудували атаку на класичну криптосистему RSA. Показано, як факторизувати число $n = pq$ за поліноміальний час, якщо відома деяка кількість наймолодших значущих біт секретних параметрів p та q. Також в їх роботі використовувався той факт, що прості числа мають спеціальну структуру, а саме $p = a_p^r + l_p$ та $q = a_q^r + l_q$ [61]. Атака ґрунтується на знаходженні оцінок невідомих параметрів у залежності від кількості відомих бітів, а також від значення степені r. Далі буде показано, що не змінюючи умови на невідомі параметри a_q та a_p, які запропонували Гафар, Аріффін та Асболла, можна прибрати залежність від ступеня r. Особливість цієї атаки полягає у тому, що для її успіху необхідна зовсім незначна кількість значущих біт секретних чисел, у порівнянні з їх розмірами. Складність здійснення атаки безпосередньо залежить від значення 2^k, де k - кількість відомих біт. Зокрема, ці біти також можна спробувати отримати шляхом перебору. Введемо два означення, які необхідні для коректного обґрунтування атаки на криптосистему RSA.

Означення 2.1. Нехай $p = (a_p^r + l_p)$ та $q = (a_q^r + l_q)$ - прості числа, такі що:

1. Параметри a_p, a_q та r - цілі, додатні числа;

2. Існують такі невідомі числа x та y, що $a_p = 2^{\alpha_1}x$ та $a_q = 2^{\alpha_2}y$;

Тоді N найменшими значущими бітами числа p, де $N \leqslant \alpha_2 r$,$\alpha_1 r$ будемо називати значення: $l_p \equiv p \pmod{2^{\alpha_1 r}}$, а числа q: $l_q \equiv q \pmod{2^{\alpha_2 r}}$

Означення 2.2. Значення A будем називати достатньо малим, якщо його довжина менша за найбільше можливе значення найнижчого рівня захищеності.

Тобто достатньо мале значення - це кількість таких чисел, які можна перебрати методом грубої сили використовуючи поточні обчислювальні можливості. За рекомендацією Інституту Інформаційних Стандартів та Технологій (National Institute of Standards and Technology) вважається, що методом грубої сили можна перебрати не більше 2^{112} значень.

Розглянемо покращення наявної атаки, яке запропоновано у такій теоремі.

Теорема 2.1. *Нехай $n = pq$ - модуль криптосистеми RSA, де $p = a_p^r + l_p$ та $q = a_q^r + l_q$. Числа a_p,a_q, r - парні, цілі числа, де $a_p^{\frac{r}{2}} > 4$, $a_p < a_q < (2a_p^r + 1)^{\frac{1}{r}}$ та вважаються невідомими. Нехай $l_p \equiv p \pmod{2^r}$ та $l_q \equiv q \pmod{2^r}$ - наймолодші значущі біти чисел p та q відповідно, такі що $l_q < 2a_q^{\frac{r}{2}}$, $l_p < 2a_p^{\frac{r}{2}}$, та $\max(l_p,l_q) < 2^N$. Якщо $2^{N-1} \cdot (\sqrt{3}+1)$ - достатньо мале число (відповідно до означення 2.2), та N наймолодших значущих біт чисел p та q відомі, то модуль n можна факторизувати за поліноміальний час.*

У роботі [61] алгоритм знаходження простих нетривіальних дільників числа n, зводиться до перебору $2^{N-1} \cdot (2^{\frac{r}{2}} + 1)$ - кандидатів на значення $(a_p a_q)^{\frac{r}{2}}$. Потім складається квадратне рівняння, коренями якого будуть числа $a_p^r l_q$ та $a_q^r l_p$ за допомогою яких вже можна обчислити параметри p та q.

Використовуючи умову $a_p < a_q < (2a_p^r + 1)^{\frac{1}{r}}$ можна покращити оцінку $2^{N-1} \cdot (2^{\frac{r}{2}} + 1)$, так що вона не буде залежати від значення r. Що і було запропоновано в теоремі 2.1. Для її доведення необхідно ввести дві допоміжні леми, які в подальшому будуть корисні для оцінок складності атак на криптосистему RSA та її модифікації.

Лема 2.1. *[61] Нехай x, $l_x \in \mathbb{Z}_+$, $r \geqslant 2$ - парне, ціле число. Якщо $\sqrt{x^r + l_x} = x^{\frac{r}{2}} + \varepsilon$, тоді $\varepsilon < \frac{l_x}{2} x^{\frac{-r}{2}}$.*

Далі використовуючи оцінку з леми 2.1 знайдемо межі значення невідомого параметра $(a_p a_q)^{\frac{r}{2}}$.

Лема 2.2. *Нехай $n = (a_p^r + l_p)(a_q^r + l_q)$, де a_p, $a_q \in \mathbb{Z}_+$, $r \geqslant 2$ - парне, ціле число. Якщо $a_p < a_q < (2a_p^r + 1)^{\frac{1}{r}}$ та при цьому: $l_p < 2a_p^{\frac{r}{2}}$ та $l_q < 2a_q^{\frac{r}{2}}$, тоді справедлива оцінка: $\sqrt{n} - (\frac{\sqrt{3}}{2} l_p + \frac{1}{2} l_q + 1) < (a_p a_q)^{\frac{r}{2}} < \sqrt{n} - \min(l_q,l_p)$*

Доведення. Оцінимо значення кореня модуля криптосистеми RSA

зверху :

$$\sqrt{n} = \sqrt{(a_p^r + l_p)(a_q^r + l_q)} < \left(a_p^{\frac{r}{2}} + \frac{l_p}{2} a_p^{\frac{-r}{2}}\right)\left(a_q^{\frac{r}{2}} + \frac{l_q}{2} a_q^{\frac{-r}{2}}\right) =$$

$$= (a_p a_q)^{\frac{r}{2}} + \left(\frac{a_q}{a_p}\right)^{\frac{r}{2}} \frac{l_p}{2} + \left(\frac{a_p}{a_q}\right)^{\frac{r}{2}} \frac{l_q}{2} + \frac{l_q l_p}{4} (a_p a_q)^{\frac{-r}{2}} <$$

$$< (a_p a_q)^{\frac{r}{2}} + \left(\frac{(2a_p^r + 1)^{\frac{1}{r}}}{a_p}\right)^{\frac{r}{2}} \frac{l_p}{2} + (1)^{\frac{r}{2}} \frac{l_q}{2} + 1 =$$

$$= (a_p a_q)^{\frac{r}{2}} + \left(\frac{(2a_p^r + 1)^{\frac{r}{r}}}{a_p^r}\right)^{\frac{1}{2}} \frac{l_p}{2} + \frac{l_q}{2} + 1 = (a_p a_q)^{\frac{r}{2}} + \left(2 + \frac{1}{a_p^r}\right)^{\frac{1}{2}} \frac{l_p}{2} + \frac{l_q}{2} + 1 <$$

$$< (a_p a_q)^{\frac{r}{2}} + \frac{\sqrt{3}}{2} l_p + \frac{1}{2} l_q + 1$$

Отже, $\sqrt{n} - (a_p a_q)^{\frac{r}{2}} < \frac{\sqrt{3}}{2} l_p + \frac{1}{2} l_q + 1 \Rightarrow (a_p a_q)^{\frac{r}{2}} > \sqrt{n} - \left(\frac{\sqrt{3}}{2} l_p + \frac{1}{2} l_q + 1\right)$

Далі оцінимо корінь знизу: $\sqrt{n} = \sqrt{(a_p a_q)^r + a_p^r l_q + a_q^r l_p + l_p l_q}$

Зауважимо, що:

$$\left(\sqrt{a_p^r l_q} - \sqrt{a_q^r l_p}\right)^2 = a_p^r l_q + a_q^r l_p - 2\sqrt{(a_p a_q)^r l_q l_p} > 0 \Rightarrow$$

$$\Rightarrow a_p^r l_q + a_q^r l_p > 2\sqrt{(a_p a_q)^r l_q l_p}$$

Тому маємо:

$$\sqrt{n} = \sqrt{(a_p a_q)^r + a_p^r l_q + a_q^r l_p + l_p l_q} > \sqrt{(a_p a_q)^r + 2\sqrt{(a_p a_q)^r l_q l_p} + l_p l_q} =$$

$$= \sqrt{\left((a_p a_q)^{\frac{r}{2}} + \sqrt{l_q l_p}\right)^2} = (a_p a_q)^{\frac{r}{2}} + \sqrt{l_q l_p} > (a_p a_q)^{\frac{r}{2}} + \min(l_q, l_p)$$

Отже, $\sqrt{n} - (a_p a_q)^{\frac{r}{2}} > \min(l_q, l_p) \Rightarrow (a_p a_q)^{\frac{r}{2}} < \sqrt{n} - \min(l_q, l_p)$

□

Далі наведемо доведення теореми 2.1.

Доведення. Оцінимо потужність множини можливих значень невідомого числа $\sqrt{(a_p a_q)^r}$. Відповідно до леми 2.2, кількість кандидатів

не перевищує:

$$\sqrt{n} - \min(l_q,l_p) - \sqrt{n} + (\frac{\sqrt{3}}{2}l_p + \frac{1}{2}l_q + 1) < 2^{N-1}(\sqrt{3}+1) - \min(l_q,l_p) + 1$$

Так як число $2^{N-1}(\sqrt{3}+1)$ достатньо мале, то застосовуючи метод грубої можна знайти значення $\sqrt{(a_p a_q)^r}$. Знаходимо значення виразу $(a_p^r l_q + a_q^r l_p)$: враховуючи, що $l_q < 2a_q^{\frac{r}{2}}$ та $l_p < 2a_p^{\frac{r}{2}}$, нам необхідно, щоб:

$$\frac{1}{2}a_p^r - 2a_p^{\frac{r}{2}} = \frac{1}{2}a_p^{\frac{r}{2}}\left(a_p^{\frac{r}{2}} - 4\right) > 0 \Rightarrow \text{ при } a_p^{\frac{r}{2}} > 4 \text{ маємо: } \frac{1}{2}a_p^r > 2a_p^{\frac{r}{2}}$$
$$\frac{1}{2}a_q^r - 2a_q^{\frac{r}{2}} = \frac{1}{2}a_q^{\frac{r}{2}}\left(a_q^{\frac{r}{2}} - 4\right) > 0 \Rightarrow \text{ при } a_q^{\frac{r}{2}} > 4 \text{ маємо: } \frac{1}{2}a_q^r > 2a_q^{\frac{r}{2}}$$

За умовою теореми, ці нерівності виконуються, тому для $(a_p^r l_q + a_q^r l_p)$ отримаємо, що:

$$(a_p^r l_q + a_q^r l_p) < 2a_q^{\frac{r}{2}}a_p^r + 2a_p^{\frac{r}{2}}a_q^r < \frac{1}{2}a_q^r a_p^r + \frac{1}{2}a_p^r a_q^r = (a_p a_q)^r$$

Звідки маємо:

$$(n - l_p l_q) \pmod{(a_p a_q)^r} = \left((a_p a_q)^r + (a_p^r l_q + a_q^r l_p)\right) \pmod{(a_p a_q)^r} = (a_p^r l_q + a_q^r l_p)$$

Далі розв'язуємо квадратне рівняння виду:

$$x^2 - (a_p^r l_q + a_q^r l_p)x + (a_p a_q)^r l_p l_q = 0$$

Отримуємо два корені: $x_1 = a_p^r l_q$ та $x_2 = a_q^r l_p$. Знаходимо секретні параметри:

$$p = \frac{n}{\frac{x_1}{l_q} + l_p}, q = \frac{n}{\frac{x_2}{l_p} + l_q}$$

□

У доведенні видно, що основна обчислювальна робота полягає в переборі $2^{N-1}(\sqrt{3}+1)$ значень, де N - кількість відомих наймолодших значущих біт. Тому складність можна оцінити, як $O(2^{N-1})$. У [61] описується приклад для 2048-бітного модуля RSA, де кількість відомих

бітів кожного з простих чисел дорівнює 12. Отже, у цьому випадку вимагається перебір $2^{11}(\sqrt{3}+1) < 5596$ - значень, який для сучасних обчислювальних можливостей виконується дуже швидко.

Запропонована атака також може використовуватись для всіх криптосистем типу RSA, стійкість яких базується на складності задачі факторизації та модуль складається з двох простих чисел p та q спеціального виду. Наприклад, до криптосистеми $RebalancedRSA$ та N-адичного розширення криптосистеми RSA дана атака застосовна.

2.2 Формальний опис криптосистеми PP-RSA

Розглянемо більше детально криптосистему $PP-RSA$, яку запропонував Т. Такагі у 1998 році. Від класичної криптосистеми RSA, модифікація відрізняється тим, що використовує модуль $n = p^k q$, та має більш складний алгоритм розшифрування.

1. **Етап створення ключів:**

1) Нехай p та $q \in \mathbb{Z}_+$ - різні прості числа приблизно однакової довжини;

2) Обираємо число k та обчислюємо $n = p^k q$ і $L = \text{НСК}(p-1,q-1)$;

3) Обираємо таке число e, щоб $\text{НСД}(e,L) = 1$ та $\text{НСД}(e,p) = 1$;

4) Обчислюємо число $d = e^{-1} \pmod{L}$ - обернене до e за модулем числа L.

Маємо (e,n) - відкритий ключ та (p,q,L,d) - секретний ключ.

2. **Шифрування:** Якщо відкритий текст $M \in \mathbb{Z}_n^*$, то:

1) $M^e \pmod{n}) = C$ - шифротекст.

3. **Розшифрування:** Нехай $M_p = M \pmod{p^k}$ та $M_q = M \pmod{modq}$:

1) M_q знаходимо як: $M_q \equiv C^d \pmod{q}$;

2) M_p знаходимо за алгоритмом розшифрування [30];

3) Далі використовуючи наслідок з Китайської теореми про лишки обчислюємо: $u = (p^k)^{-1} \pmod{q}$ та $v = q^{-1} \pmod{p^k}$, та маємо

відкритий текст: $M = (up^k M_p + vqM_q) \pmod{n}$.

Головною метою побудови цієї криптосистеми є більш швидке розшифрування. Пришвидшення відбувається, по-перше, за рахунок можливості використання секретних параметрів меншої довжини. По-друге, у алгоритмі розшифрування використовується відкрита експонента e, що робить розшифрування еквівалентним за часом шифруванню. Зокрема, для модуля довжини 1024 бітів розшифрування відбувається майже в 3,5 рази швидше.

Незважаючи, на можливість використання простих чисел меншої довжини в криптосистемі $PP - RSA$, обирати секретні параметри необхідно з урахуванням складності найшвидших існуючих алгоритмів факторизації.

Отримати значущі біти секретних параметрів можливо за допомогою різних атак по побічному каналу. Зокрема, існують методи аналізу використаних ресурсів пристрою за допомогою яких, можна отримати певну інформацію про секретні ключі RSA. Ресурси які витрачає обчислювальний пристрій під час роботи напряму залежать від інтенсивності різних частин апаратного забезпечення. Таким чином, це дає можливість отримати певну інформацію про виконувані операції та дані, які обробляються [62] .

2.3 Побудова атаки на криптосистему PP-RSA

Побудуємо розширення атаки, яку запропонували Гафар та інші у 2020 році [61]. Нехай $n = p^k q$ - модуль криптосистеми $PP - RSA$, та секретні параметри мають вигляд $p = a_p^{\frac{r}{k}} + l_p$, а $q = a_q^r + l_q$. Нехай числа $l_p \equiv p \pmod{2^{\alpha_1 \frac{r}{k}}}$ та $l_q \equiv q \pmod{2^{\alpha_2 r}}$ - це наймолодші значущі біти чисел p та q відповідно, які нам відомі. Тоді для запропонованого модуля з урахуванням деяких додаткових умов можна побудувати атаку, яка дозволить факторизувати число n за реальний час. Атака можлива за

рахунок того, що за допомогою відомих значущих біт можна оцінити невідомі параметри таким чином, щоб їх можна було знайти методом грубої сили. Для цього доведемо дві допоміжні леми.

Лема 2.3. *Нехай $x, l_x, r \in \mathbb{Z}_+$, та r - є кратне k. Тоді виконується нерівність:*

$$\sqrt[k]{x^r + l_x} < x^{\frac{r}{k}} + \frac{l_x}{k} x^{-r\frac{(k-1)}{k}}$$

Доведення. Враховуючи, що r - кратне k та x, l_x, r - додатні цілі числа, маємо:

$$\sqrt[k]{x^r + l_x} < \sqrt[k]{x^r + l_x + \sum_{i=0}^{k-2} \frac{\mathrm{C}_k^i (x^{\frac{r}{k}})^i (l_x)^{k-i}}{(kx^{\frac{r(k-1)}{k}})^{k-i}}} =$$
$$= \sqrt[k]{(x^{\frac{r}{k}} + \frac{l_x}{k} x^{-r\frac{(k-1)}{k}})^k} = \; x^{\frac{r}{k}} + \frac{l_x}{k} x^{-r\frac{(k-1)}{k}}$$

□

Далі оцінимо значення $\sqrt[k]{n} - p\sqrt[k]{a_q^r}$ зверху та знизу.

Лема 2.4. *Нехай $n = (a_p^{\frac{r}{k}} + l_p)^k (a_q^r + l_q)$, де $a_p, a_q, r \in \mathbb{Z}_+$, r - кратне k. Якщо $\max(a_p, a_q) < (2\min(a_q, a_p)^r + 1)^{\frac{1}{r}}$ та $l_q < k a_q^{r\frac{(k-1)}{k}}$, тоді справедлива оцінка: $\sqrt[k]{n} - p\sqrt[k]{a_q^r} < \frac{\sqrt[k]{3}}{2} l_q + l_p$.*

Доведення.

Враховуючи, що параметри a_p, a_q додатні числа маємо: $\sqrt[k]{n} = \sqrt[k]{\left(a_p^{\frac{r}{k}} + l_p\right)^k \left(a_q^r + l_q\right)} = \left(a_p^{\frac{r}{k}} + l_p\right) \sqrt[k]{\left(a_q^r + l_q\right)}$ застосовуючи *Лему 2.3* маємо:

$$\sqrt[k]{n} < \left(a_p^{\frac{r}{k}} + l_p\right) \left(a_q^{\frac{r}{k}} + \frac{l_q}{k} a_q^{\frac{-r(k-1)}{k}}\right) = p a_q^{\frac{r}{k}} + \frac{l_q}{k} \left(\frac{a_p}{a_q}\right)^{\frac{r}{k}} a_q^{\frac{-r(k-2)}{k}} + \frac{l_p l_q}{k} a_q^{\frac{-r(k-1)}{k}}$$

Якщо $a_p < a_q$, то враховуючи $l_q < k a_q^{r\frac{(k-1)}{k}}$, маємо:

$$\left(\frac{a_p}{a_q}\right)^{\frac{r}{k}} < 1, \; a_q^{\frac{-r(k-2)}{k}} < 1$$

і справедлива оцінка:

$$\sqrt[k]{n} - p\sqrt[k]{a_q^r} < \frac{l_q}{k} + l_p$$

Якщо, $a_q < a_p < (2a_q^r + 1)^{\frac{1}{r}}$ та $l_q < k a_q^{r\frac{(k-1)}{k}}$, то число можна оцінити як: $(\frac{a_p}{a_q})^{\frac{r}{k}} < \sqrt[k]{3}$, тому маємо:

$$\sqrt{n} - p\sqrt[k]{a_q^r} < \frac{\sqrt[k]{3}}{k} l_q + l_p$$

Оскільки параметри a_q та a_p невідомі, то візьмемо максимальне значення з двох одержаних.

□

Зауважимо, що $\sqrt[k]{n} = \sqrt[k]{p^k q} = p\sqrt[k]{q} = p\sqrt[k]{(a_q^r + l_q)} > p\sqrt[k]{a_q^r}$ з чого випливає, що $\sqrt{n} - p\sqrt[k]{a_q^r} > 0$.

Далі, сформулюємо теорему, за допомогою якої можна факторизувати модуль n.

Теорема 2.2. *Нехай $n = p^k q$ - модуль криптосистеми $PP - RSA$, де $p = a_p^{\frac{r}{k}} + l_p$ та $q = a_q^r + l_q$. Числа $a_p, a_q, r \in \mathbb{Z}_+$, де $\max(a_p,a_q) < (2\min(a_q,a_p)^r + 1)^{\frac{1}{r}}$ та вважаються невідомими. Нехай $l_p \equiv p \pmod{2^{\frac{r}{k}}}$ та $l_q \equiv q \pmod{2^r}$ - наймолодші значущі біти чисел p та q відповідно, такі що $l_q < k a_q^{r\frac{(k-1)}{k}}$ та $\max(l_p,l_q) < 2^N$. Якщо $\left(\frac{\sqrt[k]{3}}{k} + 1\right) \cdot 2^N$ — достатньо мале число (відповідно до означення 2.2), та N наймолодших значущих біт чисел p та q відомі, то модуль n можна факторизувати за час $O(2^N)$.*

Доведення.

Оцінимо значення невідомого числа $p\sqrt[k]{a_q^r}$. Відповідно до *Леми 2.4*

$$0 < \sqrt[k]{n} - p\sqrt[k]{a_q^r} < \frac{\sqrt[k]{3}}{k} l_q + l_p \tag{2.1}$$

Тоді з (2.1) отримуємо, що:

$$\sqrt[k]{n} - \frac{\sqrt[k]{3}}{k} l_q - l_p < p\sqrt[k]{a_q^r} < \sqrt[k]{n}$$

Так як, r ділиться на k, то кількість кандидатів на значення невідомого параметра $p\sqrt[k]{a_q^r}$ скічена, і оцінюється як:

$$\sqrt[k]{n} - \left(\sqrt[k]{n} - \frac{\sqrt[k]{3}}{k}l_q - l_p\right) = \frac{\sqrt[k]{3}}{k}l_q + l_p$$

Враховуючи, що $\max(l_p, l_q) < 2^N$, маємо:

$$\frac{\sqrt[k]{3}}{k}l_q + l_p < 2^N \cdot \left(\frac{\sqrt[k]{3}}{k} + 1\right)$$

Отже, якщо число $2^N \cdot \left(\frac{\sqrt[k]{3}}{k} + 1\right)$ достатньо мале, то це дає можливість знайти значення $p\sqrt[k]{a_q^r}$ шляхом грубого перебору. Далі отримавши $(p\sqrt[k]{a_q^r})^k = p^k a_q^r$, робимо обчислення:

$n - p^k a_q^r = p^k q - p^k a_q^r = p^k(a_q^r + l_q - a_q^r) = p^k l_q$ враховуючи те що l_q відоме значення маємо:

$$\frac{n - p^k a_q^r}{l_q} = p^k$$

Таким чином отримуємо секретні параметри $p = \sqrt[k]{p^k}$ та $q = \frac{n}{p^k}$.

□

Наведемо покроковий алгоритм за допомогою якого, можна знайти нетривіальні прості дільники числа n.

Алгоритм 2.1.

Вхід: n, r_p, r_q

Вихід: p, q

1: Покласти $i := \left\lfloor\left(\sqrt[k]{n} - \frac{\sqrt[k]{3}}{k}l_q - l_p\right)\right\rfloor$

2: **Поки** $i < \lceil\sqrt[k]{n}\rceil$ **виконати**:

3: | Покласти $b := (n - i^k)$

4: | Обчислити $x := \frac{b}{l_q}$

5: | **Якщо** $\sqrt[k]{x}$ - ціле число **тоді**:

6: | | Покласти $p := \sqrt[k]{x}$, $q := \frac{n}{x}$

7: | **Кінець**

5: | **Інакше:**

6: | | $i := i + 1$

7: | **Кінець**

8: **Кінець**

Зауваження. Для запобігання атаки [40] на криптосистему $PP - RSA$, число k повинно бути суттєво меншими бітової довжини секретного ключа p, у той час як довжина p повинна дорівнювати приблизно $\frac{log_2 n}{k+1}$.

Оцінимо складність запропонованого алгоритму. За одну ітерацію піднесення до степені k за схемою Горнера необхідно $\lceil log_2 k \rceil$ піднесень до квадрату та $\lceil log_2 k \rceil$ множень у найгіршому випадку. Потім необхідно одне ділення, та одне взяття кореня k-того степеня. Так як $2\lceil log_2 k \rceil$ набагато менше $2\lceil log_2(log_2 p) \rceil = o(log_2 p)$, то всі операції всередині циклу можна оцінити як $o(n)$. Максимальна кількість ітерацій дорівнює $2^N \cdot \left(\frac{\sqrt[k]{3}}{k} + 1\right) < 2^{N+1} < n^\alpha$, де $0 < \alpha < 1$. Отже, час роботи алгоритму у найгіршому випадку оцінюється як $O(n^\alpha)$.

Отже, складність даної атаки повність залежить від кількості відомих бітів секретних ключів криптосистеми $PP - RSA$ та від їхнього вигляду. Далі у підрозділі 2.6 буде оцінена кількість простих чисел виду $x^k + r$, де r - наймолодші значущі біти числа.

2.4 Опис криптосистеми GPP-RSA

Як було зазначено у розділі 1 криптосистему $GPP - RSA$ запропонували у 2000 році, і вона є узагальненням криптосистеми $PP - RSA$. Будується вона наступним чином:

1. **Етап створення ключів:**

1) Випадково обираємо p та $q \in \mathbb{Z}_+$ - різні прості числа приблизно однакової довжини;

2) Обираємо степені k,l таким чином, щоб: НСД(k,l) $= 1$ та

обчислюємо $n = p^k q^l$ і $L = \text{НСК}(p-1, q-1)$;

3) Обираємо відкриту експоненту e, щоб $\text{НСД}(e,L) = \text{НСД}(e,n) = 1$;

4) Обчислюємо секретну експоненту $d = e^{-1} \pmod{L}$.

Маємо (e,n) - відкритий ключ та (p, q, L, d) - секретний ключ.

2. **Шифрування:** Якщо відкритий текст $M \in \mathbb{Z}_n^*$, то:

1) $M^e \pmod{n} = C$ - шифротекст.

3. **Розшифрування:** Якщо $M_p = M \pmod{p^k}$ та $M_q = M \pmod{q^l}$:

1) M_p та M_q знаходимо за алгоритмом розшифрування [31];

2) Далі використовуючи наслідок з Китайської теореми про лишки обчислюємо: $u = (p^k)^{-1} \pmod{q^l}$ та $v = (q^l)^{-1} \pmod{p^k}$, та маємо відкритий текст: $M = (up^k M_p + vq^l M_q) \pmod{n}$.

Відповідно до твердження 1.2, якщо степені простих чисел модуля будуть мати вигляд, наприклад k та $k+1$, або $k-1$ та $k+1$, то шифрування буде найбільш швидким з усіх можливих модифікацій криптосистеми RSA зі складеним модулем. Тому варто розглянути чи є застосовною атака з використанням найменших значущих бітів простих чисел, які мають спеціальний вигляд до криптосистеми $GPP - RSA$.

2.5 Побудова атаки на криптосистему GPP-RSA

Нехай $n = p^k q^l$ - модуль криптосистеми $GPP - RSA$, та $p = x^r + l_p$, $q = y^r + l_q$ - секретні параметри криптосистеми, такі, що $l_p \equiv p \pmod{2^r}$ та $l_q \equiv q \pmod{2^r}$ - наймолодші значущі біти простих чисел p та q, а степінь r ділиться на добуток lk. Наступна теорема описує розширення атаки [61] на криптосистему $GPP - RSA$.

Теорема 2.3. *Нехай $n = p^k q^l$ - модуль криптосистеми $GPP-RSA$, де $p = x^r + l_p$ та $q = y^r + l_q$. Числа $x, y, r \in \mathbb{Z}_+$, де $l < k$ і $y < x < (2y^r + 1)^{\frac{1}{r}}$ та значення x, y, r вважаються невідомими. Нехай $l_p \equiv p \pmod{2^r}$ та*

$l_q \equiv q \pmod{2^r}$) - *наймолодші значущі біти чисел* p *та* q *відповідно, такі що:* $l_q < ky^{r\frac{(k-1)}{k}}$, $l_p < lx^{r\frac{(l-1)}{l}}$ *та* $\max(l_p,l_q) < 2^N$. *Якщо:*

$$2^{m-1} < \max\left(x^{\frac{r}{l}},y^{\frac{r}{k}}\right) < 2^m$$

та

$$3 \cdot \left(\frac{k + l\sqrt[l]{3}}{lk}\right) \cdot 2^{N+m}$$

— достатньо мале число (відповідно до означення 2.2), та N *наймолодших значущих біт чисел* p *та* q *відомі, то модуль* n *можна факторизувати за час* $O(2^{N+m})$.

Доведення.

Використовуючи *Лему 2.3* оцінимо значення $x^{\frac{r}{l}}y^{\frac{r}{k}}$ знизу:

$$\sqrt[kl]{n} = \sqrt[kl]{(x^r + l_p)^k(y^r + l_q)^l} = \sqrt[l]{(x^r + l_p)}\sqrt[k]{(y^r + l_q)} <$$
$$< \left(x^{\frac{r}{l}} + \frac{l_p}{lx^r}x^{\frac{r}{l}}\right)\left(y^{\frac{r}{k}} + \frac{l_q}{ky^r}y^{\frac{r}{k}}\right) = x^{\frac{r}{l}}y^{\frac{r}{k}} + \frac{x^{\frac{r}{l}}y^{\frac{r}{k}}}{x^r}\frac{l_p}{l} + \frac{x^{\frac{r}{l}}y^{\frac{r}{k}}}{y^r}\frac{l_q}{k} +$$
$$+ \frac{l_p l_q}{lk}\frac{x^{\frac{r}{l}}y^{\frac{r}{k}}}{x^r y^r} < x^{\frac{r}{l}}y^{\frac{r}{k}} + \left(\frac{y}{x}\right)^{\frac{r}{k}}\frac{x^{\frac{r}{l}}x^{\frac{r}{k}}}{x^r}\frac{l_p}{l} + \left(\frac{x}{y}\right)^{\frac{r}{l}}\frac{y^{\frac{r}{k}}y^{\frac{r}{l}}}{y^r}\frac{l_q}{k} + 1$$

Спочатку оцінимо множники $\frac{x^{\frac{r}{l}}x^{\frac{r}{k}}}{x^r}$ та $\frac{y^{\frac{r}{k}}y^{\frac{r}{l}}}{y^r}$:

Якщо $1 < l < k$, то : $lk - (l+k) = k(l-1) - l > l(l-1) - l = l(l-2) \geqslant 0 \Rightarrow$

$$\Rightarrow \frac{(l+k)}{lk} < 1 \Rightarrow \frac{(l+k)}{lk}r < r \Rightarrow \frac{x^{\frac{(l+k)}{lk}r}}{x^r} < 1$$

Аналогічно отримуємо, що:

$$\frac{y^{\frac{(l+k)}{lk}r}}{y^r} < 1$$

Далі, враховуючи що $y < x < (2y^r + 1)^{\frac{1}{r}}$ маємо:

$$\left(\frac{y}{x}\right)^{\frac{r}{k}} < 1$$

$$\left(\frac{x}{y}\right)^{\frac{r}{l}} < \left(\frac{(2y^r+1)^{\frac{1}{r}}}{y}\right)^{\frac{r}{l}} = \left(\frac{2y^r+1}{y^r}\right)^{\frac{1}{l}} < \sqrt[l]{3}$$

Остаточно отримуємо:

$$\sqrt[kl]{n} < x^{\frac{r}{l}}y^{\frac{r}{k}} + \frac{l_p}{l} + \frac{\sqrt[l]{3}}{k}l_q + 1 \Rightarrow x^{\frac{r}{l}}y^{\frac{r}{k}} > \sqrt[kl]{n} - \frac{l_p}{l} - \frac{\sqrt[l]{3}}{k}l_q - 1$$

Зверху значення $x^{\frac{r}{l}}y^{\frac{r}{k}}$ оцінюється як:

$$\sqrt[kl]{n} = \sqrt[kl]{(x^r+l_p)^k(y^r+l_q)^l} > \sqrt[kl]{(x^r)^k(y^r)^l} = x^{\frac{r}{l}}y^{\frac{r}{k}}$$

Так як $\frac{r}{l}$ та $\frac{r}{k}$ - цілі числа, то кількість кандидатів на невідоме значення $x^{\frac{r}{l}}y^{\frac{r}{k}}$, не перевищує:

$$\sqrt[kl]{n} - (\sqrt[kl]{n} - \frac{l_p}{l} - \frac{\sqrt[l]{3}}{k}l_q - 1) = \frac{l_p}{l} + \frac{\sqrt[l]{3}}{k}l_q + 1 < 2^N\left(\frac{k+l\sqrt[l]{3}}{lk}\right) + 1$$

За умовою, $2^N\left(\frac{k+l\sqrt[l]{3}}{lk}\right)$ достатньо мале число, отже зможемо знайти невідоме значення методом перебору.

Далі, оцінимо значення суми $x^{\frac{r}{l}} + y^{\frac{r}{k}}$:

$$\max\left(x^{\frac{r}{l}},y^{\frac{r}{k}}\right) < x^{\frac{r}{l}} + y^{\frac{r}{k}} < 2\max\left(x^{\frac{r}{l}},y^{\frac{r}{k}}\right)$$

За умовою $2^{m-1} < \max\left(x^{\frac{r}{l}},y^{\frac{r}{k}}\right) < 2^m$, тоді отримаємо, що: $2^{m+1} - 2^{m-1} = 2^{m-1}(2^2-1) = 3\cdot 2^{m-1}$ - за умовою достатньо мале число, тоді методом перебору знайдемо значення суми $x^{\frac{r}{l}} + y^{\frac{r}{k}}$.

Далі складаємо квадратне рівняння:

$$z^2 - (x^{\frac{r}{l}} + y^{\frac{r}{k}})z + x^{\frac{r}{l}}y^{\frac{r}{k}} = 0$$

і знаходимо його корені:

$$z_1 = x^{\frac{r}{l}},\ z_2 = y^{\frac{r}{k}}$$

Звідки маємо: $p = (z_1)^l + l_p$ та $q = (z_2)^k + l_q$ - секретні ключі криптосистеми.

□

Побудуємо алгоритм факторизації модуля $n = p^k q^l$:

Алгоритм 2.2.

Вхід: n, r_p, r_q, m

Вихід: p, q

1: Покласти $i := \left\lfloor \left(\sqrt[kl]{n} - \frac{l_p}{l} - \frac{\sqrt[l]{3}}{k} l_q - 1 \right) \right\rfloor$

2: **Поки** $i < \lceil \sqrt[kl]{n} \rceil$ **виконати**:

3: | $j := 2^{m-1}$

4: | **Поки** $j < 2^{m+1}$ **виконати**:

5: | **Розв'язати рівняння:** $z^2 - j \cdot z + i = 0$:

6: | Покласти $x_1 := z_1$, $x_2 := z_2$

7: | **Якщо** $Q := \frac{n}{((x_1)^k + l_q)^l}$ - ціле число **тоді**:

8: | | $p := (x_2)^l + l_p, q := (x_1)^k + l_q$

9: | | **Вихід**

10: | **АБО Якщо** $P := \frac{n}{((x_1)^l + l_p)^k}$ - ціле число **тоді**:

11: | | $p := (x_1)^l + l_p, q := (x_2)^k + l_q$

12: | | **Вихід**

13: | **Інакше:**

14: | | $j := j + 1$

15: | **Кінець**

16: | $i := i + 1$

17: **Кінець**

Отже, можливість здійснення атаки дуже сильно залежить від кількості відомих бітів, а також від довжини простих чисел, які є дільниками модуля. Тому часову складність алгоритму можна оцінити як $O(2^{N+m})$. Розглянемо приклад, який проілюструє можливі значення числа $3 \cdot 2^{N+m} \left(\frac{k + l\sqrt[l]{3}}{lk} \right)$.

Приклад 2.1. Нехай $n = p^4 q^3$ - модуль криптосистеми $GPP - RSA$

бітова довжина якого дорівнює 2048 (такий варіант модуля пропонується у [31]), припустимо, що прості числа мають вид: $p = x^r + l_p$ та $q = y^r + l_q$. Звідси маємо що:

$$\|p\| \approx \|q\| = \frac{2048}{4+3} \approx 293$$

Тоді, $x^r \approx 2^{293}, y^r \approx 2^{293} \Rightarrow x^{\frac{r}{3}} < 2^{98}$, а $y^{\frac{r}{4}} < 2^{73}$. Отже, значення:

$$3 \cdot 2^{N+m} \left(\frac{k + l\sqrt[l]{3}}{lk} \right) < 3 \cdot 2^{N+98} \left(\frac{4 + 3\sqrt[3]{3}}{12} \right) \approx 2^{N+99}$$

Для того, щоб 2^{N+99} було достатньо малим, необхідно щоб $N < 13$. Тобто кількість відомих бітів не повинна перевищувати 13, що цілком можливо.

Треба відзначити, що у порівнянні зі складністю атаки на криптосистему $PP - RSA$, ця атака є набагато менш ефективною та фактично вимагає перебору 2^{N+m}, де 2^m для невеликих степенів k та l для реального модуля $GPP - RSA$ не завжди буде достатньо малим значенням. Розглянемо варіант криптосистеми $GPP - RSA$, коли довжина модуля дорівнює 2048 біт, а степені простих чисел дорівнюють 3 та 2. Отримаємо, що $\|p\| \approx \|q\| = \frac{2048}{5} \approx 409$, і тоді вже $x^{\frac{r}{2}} \approx 2^{204}$, а $y^{\frac{r}{3}} \approx 2^{136}$, що набагато більше за значення 2^{112} і тому перебір стає неможливим.

2.6 Обчислення оцінки кількості простих чисел, які використовуються побудованими атаками

Для того щоб оцінити ймовірність успіху наведеної атаки необхідно обчислити кількість простих чисел, які мають вигляд $a^r + l$, де r - додатне ціле число, кратне k.

Спочатку оцінимо потужність множини $B_m = \{x \in \mathbb{Z}_+ : \exists b \in \mathbb{Z}_+ : b^r = x \wedge \|x\| = m\}$ - тобто кількість чисел r-тих степенів бітова довжина яких m.

Твердження 2.1. *Нехай m - деяке додатне ціле число, тоді*

потужність множини $|B_m|$ *є не меншою ніж :*

$$\left\lfloor 2^{\frac{m-1}{r}} \left(\sqrt[r]{2} - 1\right) \right\rfloor$$

Доведення.

B_m - множина r-тих степенів чисел бітова довжина яких m. Це числа, які задовольняють нерівність:

$$2^{m-1} < b^r < 2^m \Rightarrow \sqrt[r]{2^m} < b < \sqrt[r]{2^{m-1}}$$

Далі обчислимо різницю між верхньою та нижньою межею :

$$\sqrt[r]{2^m} - \sqrt[r]{2^{m-1}} = \sqrt[r]{2^{m-1}} \left(\sqrt[r]{2} - 1\right)$$

Так як множина B_m складається з цілих чисел то її потужність не менше ніж:

$$\left\lfloor \sqrt[r]{2^{m-1}} \left(\sqrt[r]{2} - 1\right) \right\rfloor$$

□

Нехай функція $\pi(x)$ - кількість простих чисел, менших за число x. З теореми [63] відомо, що значення функції $\pi(x) \approx \frac{x}{ln(x)}$. Оцінимо кількість простих чисел виду $q = a^r + l$, довжина яких дорівнює m біт, де r - додатне ціле число, число a - парне, а значення $2^{N-1} \leqslant l < 2^N$, тобто $\|l\| = N$. Вважаємо, що $l \equiv q \pmod{2^r}$.

Нехай b - це найменше парне додатне число, таке що $\|b^r\| = m$ біт. Тоді відповідно до твердження 2.1 кількість r-тих степенів довжина яких m біт не менше $L = \left\lfloor \sqrt[r]{2^{m-1}} \left(\sqrt[r]{2} - 1\right) \right\rfloor$, і вони мають вигляд: $b^r, (b+1)^r, \ldots, (b+L-1)^r, (b+L)^r$. Розлянемо випадок, коли L парне число, тоді підходять всі числа виду: $b^r, (b+2)^r, (b+4)^r, \ldots, (b+L-2)^r, (b+L)^r$ та їхня кількість дорівнює $\frac{L}{2} + 1$. Далі кількість простих чисел між значеннями $b^r + 2^N$ та $b^r + 2^{N-1}$ оцінюється, як:

$$\pi(b^r + 2^N) - \pi(b^r + 2^{N-1}) \approx \frac{b^r + 2^N}{ln(b^r + 2^N)} - \frac{b^r + 2^{N-1}}{ln(b^r + 2^{N-1})} < \\ < \frac{b^r + 2^N}{ln(b^r)} - \frac{b^r + 2^{N-1}}{ln(b^r)} = \frac{2^{N-1}}{rln(b)}$$

Тут зроблено припущення, що число b^r достатньо велике (тобто більше ніж 2^{112}) та 2^N набагато менше ніж b^r. Відповідно для наступних чисел маємо:

$$\pi((b+2)^r + 2^N) - \pi((b+2)^r + 2^{N-1}) < \frac{2^{N-1}}{rln(b+2)}$$

$$\pi((b+4)^r + 2^N) - \pi((b+4)^r + 2^{N-1}) < \frac{2^{N-1}}{rln(b+4)}$$

$$\vdots$$

$$\pi((b+L-2)^r + 2^N) - \pi((b+L-2)^r + 2^{N-1}) < \frac{2^{N-1}}{rln(b+L-2)}$$

$$\pi((b+L)^r + 2^N) - \pi((b+L)^r + 2^{N-1}) < \frac{2^{N-1}}{rln(b+L)}$$

Тоді, кількість простих чисел виду $b^r + l$ та довжини m біт з відомими N бітами приблизно дорівнює:

$$\frac{2^{N-1}}{rln(b)} + \frac{2^{N-1}}{rln(b+2)} + \ldots + \frac{2^{N-1}}{rln(b+L)} = \frac{2^{N-1}}{r} \sum_{i=0}^{\frac{L}{2}+1} \frac{1}{ln(b+i)}$$

Далі, так як b достатньо велике число, а функція логарифму зі збільшенням аргументу починає все більше нагадувати лінійну функцію,

тоді можемо розглядати сумму, як арифметичну прогресію:

$$\frac{2^{N-1}}{r}\sum_{i=0}^{\frac{L}{2}+1}\frac{1}{ln(b+i)} \approx \frac{2^{N-1}}{r}\left(\frac{L}{2}+1\right)\cdot\frac{1}{2}\left(\frac{1}{ln(b)}+\frac{1}{ln(b+L)}\right) =$$

$$= \left(\frac{\left\lfloor \sqrt[r]{2^{m-1}}\left(\sqrt[r]{2}-1\right)\right\rfloor}{2}+1\right)\cdot\left(\frac{2^{N-2}}{ln\left(b\right)^{r}}+\frac{2^{N-2}}{ln\left(b+\left\lfloor \sqrt[r]{2^{m-1}}\left(\sqrt[r]{2}-1\right)\right\rfloor\right)^{r}}\right)$$

Якщо значення L непарне, то оцінка отримується аналогічно, але кількість доданків у сумі стає рівною $\frac{L+1}{2}$.

Для здійснення атак на криптосистеми RSA, $PP-RSA$ та $GPP-RSA$ потрібно зовсім небагато наймолодших значущих бітів. Тому для уникнення атаки на криптосистему RSA у роботі [61] було запропоновано перевіряти чи є різниця:

$$\left\lceil \sqrt{n}-\lfloor\sqrt{p}\rfloor\,\lfloor\sqrt{q}\rfloor\right\rceil$$

— достатньо маленьким числом. Якщо так — то необхідно обрати нові прості числа в якості секретних параметрів. Для випадку $PP-RSA$ та $GPP-RSA$ в залежності від модуля також слід перевіряти вигляд простих чисел. Для модуля p^kq - так само було б доречно перевіряти різницю:

$$\left\lceil \sqrt[k]{n}-p\,\lfloor\sqrt[k]{q}\rfloor\right\rceil$$

— чи є вона достатньо маленьким числом. А для секретних параметрів криптосистеми $GPP-RSA$ слід робити аналогічну перевірку в залежності від їх бітового розміру.

Висновки до розділу 2

У розділі більш детально розглянуто наявну атаку на криптосистему RSA з використанням наймолодших значущих бітів та чисел спеціального виду. Зроблено її покращення, яке дозволило швидше

факторизувати модуль та зменшити кількість необхідних даних для проведення атаки. Побудовано розширення запропонованої атаки на криптосистеми $PP - RSA$ та криптосистеми $GPP - RSA$. Для $PP - RSA$ атака виявилась набагато більш ефективною, так як її успіх залежить тільки від кількості відомих значущих біт числа та виду простих чисел. У випадку $GPP - RSA$ атака потребує набагато більше обчислювальних ресурсів, так як час роботи експоненційно залежить не тільки від кількості відомих біт, а й від довжини простих чисел. Недивлячись на те, що для криптосистеми $PP - RSA$ час роботи алгоритму факторизації модуля теж експоненційний атака може бути здійснена за реальний час. Для випадку коли відомо N - наймолодших значущих біт криптосистеми час роботи становить $O(2^N)$ - для $PP - RSA$ і $O(2^{N+m})$ для $GPP - RSA$, де значення m - залежить від довжини простих чисел та від степенів модуля криптосистеми. Оцінено кількість простих чисел фіксованої довжини, які використовуються побудованими атаками.

ВИСНОВКИ

На сьогодні RSA — одна з найпопулярніших асиметричних криптосистем у криптографії та має широке практичне застосування. Одними з важливих параметрів цього криптопримітиву є час розшифрування та довжина модуля. Це зумовило появу багатьох модифікацій криптосистеми RSA, мета яких збільшити швидкість розшифрування або зменшити довжину ключів без втрати належної стійкості.

Коротко розглянуто найбільш відомі модифікації криптосистеми RSA, такі як: $PP-RSA$, $GPP-RSA$, $MF-RSA$, $KMOV$ та інші, які побудовані для різних цілей. Розглянуті наявні атаки на криптосистему RSA та декілька атак на кожну з 4 RSA-подібних криптосистем. Більшість з них використовує відомі значущі біти секретної експоненти або припущення про розмір цієї експоненти. Багато з запропонованих атак є модифікаціями вже наявних атак на криптосистему RSA. Зокрема, не всі атаки можуть бути ефективно розширені на модифікації криптосистеми RSA. У ході дослідження:

1) Покращена наявна атака з використанням структури простих на криптосистему RSA. Складність наявної атаки оцінювалась як $O(2^{N-1} \cdot (2^{\frac{r}{2}} + 1))$ та для її здійснення вимагалось, щоб степінь r був відомим. Доведено, що степінь невідомого ключа знати не потрібно та кількість операцій буде залежати тільки від кількості відомих бітів, і часова складність оцінюється як $O(2^{N-1})$.

2) Побудована атака з використанням структури простих на криптосистему $PP-RSA$. Вона дозволяє знайти прості нетривіальні дільника модуля за час $O(2^N)$, де N - це максимальна відома кількість бітів секретних ключів криптосистеми. На відміну від наявних атак з використанням відомих бітів секретних параметрів, які потребують щоб прості числа мали спільні найстарші значущі біти, запропонована атака

буде більш ефективною, коли відомо якомога менше значущих біт. Однак, це тільки за умови, що прості числа мають певну структуру.

3) Побудована атака з використанням структури простих на криптосистему $GPP - RSA$. Складність запропонованої атаки оцінюється як $O(2^{N+m})$, де N - це максимальна відома кількість наймолодших значущих бітів секретних ключів криптосистеми, а значення m вже суттєво залежить від довжини простих чисел криптосистеми. Чим більше довжина модуля криптосистеми, тим більше значення m і відповідно тим менш ефективна атака.

4) Обчислена оцінка кількості простих чисел виду $a^r + l$, бітова довжина яких фіксована та бітова довжина значення l також фіксована. Зокрема, чим менше значення r тим більша кількість простих чисел такого виду певної довжини.

Порівнюючи атаки на криптосистеми RSA, та $PP - RSA$ та $GPP - RSA$, видно, що для однакової кількості відомих бітів найефективнішою є атака на криптосистему RSA. Зокрема, запропонована атака вимагає, щоб прості числа мали вигляд $a^r + l$, де степінь r повинен бути кратний 2 для простих чисел RSA, у той час як для криптосистеми $PP - RSA$ та $GPP - RSA$ потрібний параметр r залежить від вигляду їхніх модулів. Складність здійснення атаки на криптосистему $PP - RSA$ еквівалентна складності атаки на RSA, коли застосування атаки на $GPP - RSA$ набагато менш ефективне і взагалі не завжди можливе.

ПЕРЕЛІК ПОСИЛАНЬ

1. Bakhtiari M., Maarof M. A. Serious security weakness in RSA cryptosystem //International Journal of Computer Science Issues (IJCSI). – 2012. – Vol. 9. – №. 1. – P. 175–178.

2. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems //Communications of the ACM. – 1978. – Vol. 21. – №. 2. – P. 120-126.

3. Hastad J. Solving Simultaneous Modular Equations of Low Degree / Johan Hastad // SIAM J. Comput. – 1988. – Vol. 17. – P. 336–341.

4. Franklin M., Reiter M. A linear protocol failure for RSA with exponent three. 1995 //Rump Session of Crypto. – Vol. 95.

5. Coppersmith D. et al. Low-exponent RSA with related messages / Don Coppersmith, Matthew Franklin, Jacques Patarin, Michael Reiter //International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 1996. – P. 1-9.

6. Dubey M. K. et al. Cryptanalytic attacks and countermeasures on RSA //Proceedings of the Third International Conference on Soft Computing for Problem Solving. – Springer, New Delhi, 2014. – P. 805-819.

7. Boneh D., Durfee G. Cryptanalysis of RSA with private key d less than $N^{0.292}$ //IEEE transactions on Information Theory. – 2000. – vol. 46. – №. 4. – P. 1339-1349.

8. Blömer J., May A. A generalized Wiener attack on RSA //International Workshop on Public Key Cryptography. – Springer, Berlin, Heidelberg, 2004. – P. 1-13.

9. Blömer J., May A. New partial key exposure attacks on RSA //Annual International Cryptology Conference. – Springer, Berlin, Heidelberg, 2003. – P. 27-43.

10. Coppersmith D. Small solutions to polynomial equations, and low exponent RSA vulnerabilities //Journal of cryptology. – 1997. – vol. 10. – №.

4. – P. 233-260.

11. Dujella A. Continued fractions and RSA with small secret exponent.[електронний ресурс] //arXiv preprint cs/0402052. – 2004.— Режим доступу: https://arxiv.org/pdf/cs/0402052.pdf

12. Heninger N., Shacham H. Reconstructing RSA private keys from random key bits //Annual International Cryptology Conference. – Springer, Berlin, Heidelberg, 2009. – P. 1-17.

13. Василенко О. Н. В19 Теоретико-числовые алгоритмы в криптографии.—М.: МЦНМО, 2003.—328 с. – 2003.

14. Lenstra A. K. et al. The number field sieve //The development of the number field sieve. – Springer, Berlin, Heidelberg, 1993. – С. 11-42.

15. Kleinjung T. et al. Factorization of a 768-bit RSA modulus //Annual Cryptology Conference. – Springer, Berlin, Heidelberg, 2010. – P. 333-350.

16. Rivest R. L., Shamir A., Adleman L. M. Cryptographic communications system and method : пат. 4405829 США. – 1977.

17. Quisquater J. J., Couvreur C. Fast decipherment algorithm for RSA public-key cryptosystem //Electronics letters. – 1982. – Vol. 18. – №. 21. – P. 905-907.

18. Sahadeo Padhye. An Efficient Variant of RSA Cryptosystem.[електронний ресурс] // Cryptology ePrint Archive, Report 2005/392. – 2005. – Режим доступу: https://eprint.iacr.org/2005/392

19. Koyama K. et al. New public-key schemes based on elliptic curves over the ring Z_n //Annual International Cryptology Conference. – Springer, Berlin, Heidelberg, 1991. – P. 252-266.

20. Rabin M. O. Digitalized signatures and public-key functions as intractable as factorization. – Massachusetts Inst of Tech Cambridge Lab for Computer Science, 1979.

21. Kurosawa K., Okada K., Tsujii S. Low exponent attack against elliptic curve RSA //Information processing letters. – 1995. – vol. 53. – №. 2. – P. 77-83.

22. Demytko N. A new elliptic curve based analogue of RSA //Workshop on the Theory and Application of of Cryptographic Techniques. – Springer,

Berlin, Heidelberg, 1993. – P. 40-49.

23. Koyama K. Fast RSA-type schemes based on singular cubic curves $y^2 + axy = x^3(modn)$ //International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 1995. – P. 329-340.

24. Kuwakado H., Koyama K., Tsuruoka Y. A new RSA-type scheme based on singular cubic curves $y^2 \equiv x^3 + bx^2(modn)$ //IEICE transactions on fundamentals of electronics, communications and computer sciences. – 1995. – Vol. 78. – №. 1. – P. 27-33.

25. Shamir A. RSA for paranoids //CryptoBytes. – 1995. – Vol. 1. – P. 1-4.

26. Takagi T. Fast RSA-type cryptosystems using n-adic expansion //Annual International Cryptology Conference. – Springer, Berlin, Heidelberg, 1997. – P. 372-384.

27. Collins T. et al. Public key cryptographic apparatus and method : пат. 5848159 США. – 1998.

28. Lenstra Jr H. W. Factoring integers with elliptic curves //Annals of mathematics. – 1987. – P. 649-673.

29. Boneh D., Shacham H. Fast variants of RSA //CryptoBytes. – 2002. – Vol. 5. – №. 1. – P. 1-9.

30. Takagi T. Fast RSA-type cryptosystem modulo $p^k q$ //Annual International Cryptology Conference. – Springer, Berlin, Heidelberg, 1998. – P. 318-326.

31. Lim S. et al. A Generalized Takagi-Cryptosystem with a Modulus of the Form $p^r q^s$ //International Conference on Cryptology in India. – Springer, Berlin, Heidelberg, 2000. – P. 283-294.

32. Wiener M. J. Cryptanalysis of short RSA secret exponents //IEEE Transactions on Information theory. – 1990. – Vol. 36. – №. 3. – P. 553-558.

33. Cesar Alison Monteiro Paixão. An efficient variant of the RSA cryptosystem. [електронний ресурс] // Cryptology ePrint Archive, Report 2003/159. 2003. – Режим доступу: https://eprint.iacr.org/2003/159

34. Boudabra M., Nitaj A. A new generalization of the KMOV cryptosystem //Journal of Applied Mathematics and Computing. – 2018. – Vol. 57. – №. 1. – P. 229-245.

35. Pinch R. G. E. Extending the Wiener attack to RSA-type cryptosystems //Electronics Letters. – 1995. – Vol. 31. – №. 20. – P. 1736-1738.

36. Kaliski B. S. A chosen message attack on Demytko's elliptic curve cryptosystem //Journal of Cryptology. – 1997. – Vol. 10. – №. 1. – P. 71-72.

37. Chua S. K., Leung K. H., Ling S. Attack on RSA-type cryptosystems based on singular cubic curves over Z/nZ //Theoretical computer science. – 1999. – Vol. 226. – №. 1-2. – P. 19-27.

38. Ibrahimpasic B. Cryptanalysis of KMOV cryptosystem with short secret exponent / Bernadin Ibrahimpasic // Proceeding of the 19th Central European Conference on Information and Intelligent Systems 2008. – 2008. – P. 407–414.

39. Abderrahmane Nitaj. A new attack on the KMOV cryptosystem. [електронний ресурс] //Cryptology ePrint Archive, Report 2011/427. 2011. - Режим доступу: https://eprint.iacr.org/2011/427

40. Boneh D., Durfee G., Howgrave-Graham N. Factoring $N = p^r q$ for large r //Annual International Cryptology Conference. – Springer, Berlin, Heidelberg, 1999. – P. 326-337

41. May A. Secret Exponent Attacks on RSA-type Schemes with Moduli $N = p^r q$ //International Workshop on Public Key Cryptography. – Springer, Berlin, Heidelberg, 2004. – P. 218-230.

42. Itoh K., Kunihiro N., Kurosawa K. Small secret key attack on a variant of RSA (due to Takagi) //Cryptographers' Track at the RSA Conference. – Springer, Berlin, Heidelberg, 2008. – P. 387-406.

43. Sarkar S. Small secret exponent attack on RSA variant with modulus $N = p^r q$ //Designs, Codes and Cryptography. – 2014. – Vol. 73. – №. 2. – P. 383-392.

44. Sarkar S. Revisiting prime power RSA //Discrete Applied Mathematics. – 2016. – Vol. 203. – P. 127-133.

45. Lenstra A. K., Lenstra H. W., Lovász L. Factoring polynomials with rational coefficients //Mathematische annalen. – 1982. – Vol. 261. – №. ARTICLE. – P. 515-534.

46. Nitaj A., Rachidi T. New attacks on RSA with moduli $N = p^r q$ //International Conference on Codes, Cryptology, and Information Security. – Springer, Cham, 2015. – P. 352-360.

47. Lu Y., Zhang R., Lin D. New Results on Solving Linear Equations Modulo Unknown Divisors and its Applications. [електронний ресурс] // Cryptology ePrint Archive, Report 2014/343. 2014.

48. Esgin M. F., Kiraz M. S., Uzunkol O. A new partial key exposure attack on multi-power RSA //International Conference on Algebraic Informatics. – Springer, Cham, 2015. – P. 103-114.

49. Akchiche O., Khadir O. Factoring multi power RSA moduli with a class of secret exponents //Acta Universitatis Sapientiae, Informatica. – 2015. – Vol. 7. – №. 2. – P. 143-150.

50. Shehu S., Ariffin M. R. K. New cryptanalytic results upon prime power moduli $N = p^r q$ //AIP Conference Proceedings. – AIP Publishing LLC, 2019. – Vol. 2184. – №. 1. – P. 020011.

51. Asbullah M. A., Ariffin M. R. K. New attacks on RSA with modulus $N = p^2 q$ using continued fractions //Journal of Physics: Conference Series. – IOP Publishing, 2015. – Vol. 622. – №. 1. – P. 012019.

52. Lu Y. Cryptanalysis of an RSA variant with Moduli $N = prq$ / Yao Lu, Liqiang Peng, Santanu Sarkar // The 9th International Workshop on Coding and Cryptography 2015 WCC2015. – 2015.

53. Coron J. S. et al. Facto ring $N = p^r q^s$ for large r and s //Cryptographers' Track at the RSA Conference. – Springer, Cham, 2016. – P. 448-464.

54. Mengce Zheng. Improved Results on Factoring General RSA Moduli with Known Bits. [електронний ресурс] // Cryptology ePrint Archive, Report 2018/609. 2018. - Режим доступу: https://eprint.iacr.org/2018/609

55. Ciet M. et al. Short private exponent attacks on fast variants of

RSA //UCL Crypto Group Technical Report Series CG-2002/4, University Catholique de Louvain. – 2002. – P. 1À24.

56. Hinek M. J., Low M. K., Teske E. On some attacks on multi-prime RSA //International Workshop on Selected Areas in Cryptography. – Springer, Berlin, Heidelberg, 2003. – P. 385-404.

57. Hinek M. J. On the security of multi-prime RSA //Journal of Mathematical Cryptology. – 2008. – Vol. 2. – №. 2. – P. 117-147.

58. Zhang H., Takagi T. Attacks on multi-prime RSA with small prime difference //Australasian Conference on Information Security and Privacy. – Springer, Berlin, Heidelberg, 2013. – P. 41-56.

59. Zheng M., Kunihiro N., Hu H. Improved factoring attacks on multi-prime RSA with small prime difference //Australasian Conference on Information Security and Privacy. – Springer, Cham, 2017. – P. 324-342.

60. Adenan N. N. H. et al. New Jochemsz–May Cryptanalytic Bound for RSA System Utilizing Common Modulus $N = p^2q$ //Mathematics. – 2021. – Vol. 9. – №. 4. – P. 340.

61. Abd Ghafar A. H., Kamel Ariffin M. R., Asbullah M. A. A New LSB Attack on Special-Structured RSA Primes //Symmetry. – 2020. – Vol. 12. – №. 5. – P. 838.

62. Kocher P. et al. Introduction to differential power analysis //Journal of Cryptographic Engineering. – 2011. – Vol. 1. – №. 1. – P. 5-27.

63. Jameson G. J. O. The prime number theorem. – Cambridge University Press, 2003. – №. 53.