Міністерство освіти і науки України
Національний університет «Києво-Могилянська академія»
Факультет інформатики
Кафедра математики

Кваліфікаційна робота
освітній ступінь – магістр

на тему: **«СХЕМА РОЗПОДІЛУ СЕКРЕТНИХ КЛЮЧІВ КРИПТОСИСТЕМИ ГОЛДВАССЕР-ГОЛДРІХА-ХАЛЕВІ»**

Виконав: студент 2-го року навчання
магістерської освітньої програми «Прикладна математика», спеціальності 113 Прикладна математика

Ліхачов Артемій Дмитрович

Керівник: Олійник Б.В.
професор, д.ф-м. наук

Рецензент: .

Магістерський проект захищений з оцінкою

_____

Секретар
ЕК_____
(підпис)
«_____» _____
20___р.

Київ - 2024

Зміст

Анотація

Кваліфікаційна робота присвячена розробці схеми розподілення секрету, що базується на криптосистемі Голдвассер-Голдріха-Халеві. Робота складається зі вступу, трьох розділів, висновку та списку використаної літератури. У вступі розповідається про актуальність дослідження. У першому розділі наводяться означення решітки, формулюються задачі пошуку найкоротшого вектору, найближчого вектору та найменшого базису, наводиться алгоритм Бабаї. У другому розділі розглядається криптосистема Голдвассер-Голдріха-Халеві. У третьому розділі наводиться визначення схеми розподілу секрету та вимог до неї, описується схема на криптосистемі Голдвассер-Голдріха-Халеві, формулюється та доводиться теорема щодо її коректності та статистичної конфіденційності, наводиться відповідний приклад. У висновку підсумовуються отримані результати проєкту.

Ключові слова: *цілочисельні решітки, алгоритм Бабаї, криптосистема Голдвассер-Голдріха-Халеві, схеми розподілу секрету, асиметричні алгоритми шифрування*

Вступ

З розвитком квантових технологій стає актуальним питання про дослідження та впровадження криптосистем, що базуватимуться на складних задачах для квантових обчислень. Прикладом таких задач, що мають експоненційну складність для квантових обчислень, є задачі на решітках такі як пошук найкоротшого вектора або пошук найближчого вектора. Криптографічні системи та протоколи, які мають зазначені задачі в основі свого математичного апарату є стійкими до квантового криптоаналізу [1],[2].

Схема розподілення секрету [3] є фундаментальним криптографічним примітивом що допускає розподілення секрету між множиною учасників, при цьому відновлення секрету можливе тільки при авторизації всіх або певної частини учасників (порогу учасників). Також необхідною умовою схеми розподілення секрету є неможливість окремих учасників, або груп учасників, кількість яких менша за поріг, відновити секрет.

Варіанти побудови схем розподілу секрету на різних математичних моделях[4], у тому числі й на решітках [5], наразі активно досліджуються різними науковцями. У даній роботі запропоновано нову n-порогову схему розподілу секрету для n учасників, що базується на криптосистемі Голдвассер-Голдріха-Халеві.

Робота складається з 3 розділів. У першому розділі наводяться необхідні означення та теореми для подальшого дослідження криптосистеми на основі решіток. Другий розділ наводить визначення криптосистеми Голдвассер-Голдріха-Халеві. Третій розділ складається з двох частин і містить опис схеми розподілів секрету та її застосування на основі криптосистеми Голдвассер-Голдріха-Халеві.

Об’єкт дослідження – асиметричні методи та алгоритми шифрування.

Предмет дослідження – схеми розподілу секрету та цілочисельні решітки.

Мета дослідження – побудова нової схеми розподілу секрету, що базується на складній задачі на решітках.

Методи дослідження – основні методи, що використані в роботі є методами криптографічного аналізу та теорії решіток.

Розділ 1

Необхідні визначення

У цьому розділі наведено основні означення, що використовуватимуться впродовж роботи.

Означення 1.1. *[1] Нехай $v_1, \ldots, v_n \in \mathbb{R}^m$ є множиною лінійно незалежних векторів. Решіткою L породженою $v_1, \ldots, v_n$ називається множина всіх лінійних комбінацій $v_1, \ldots, v_n$ з цілими коефіцієнтами, тобто*

$$L = \{a_1 v_1 + a_2 v_2 + \ldots + a_n v_n \mid a_1, a_2, \ldots, a_n \in \mathbb{Z}\}.$$

В основі задач на решітках лежать поняття про "хороший" та "поганий" базиси. Далі наведено відповідне означення.

Означення 1.2. *[1] "Поганим" базисом решітки L називають менш ортогональний базис решітки.*

На наступному рисунку синім кольором зображено "поганий" базис, а червоним - "хороший" базис.

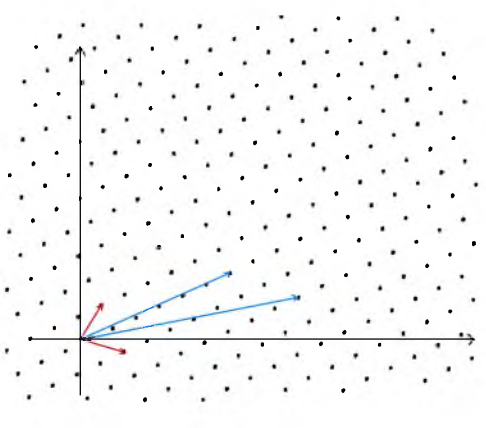

Рис. 1.1: Двовимірна решітка із різними базисними векторами

Далі будуть наведені визначення основних складних задач на решітках: пошук найкоротшого вектору, пошук найближчого вектору та пошук найменшого базису.

Означення 1.3. *[1] Проблему пошуку найкоротшого вектору (Shortest Vector Problem, SVP), у решітці L можна описати одним із трьох наступних способів:*

- *знайти ненульовий вектор x у решітці L, для котрого*

$$\|x\| \leq \|y\|$$

для всіх ненульових $y \in L$, тобто $\|x\| = \lambda_1(L)$.

- *SVP_γ: знаходження апроксимованого найменшого вектора x у решітці L, який*

$$\|x\| \leq \gamma \cdot \lambda_1(L),$$

для малої константи γ.

- *$uSVP_\gamma$: для константи $\gamma > 1$ та решітки L таких, що*

$$\lambda_2(L) > \gamma \cdot \lambda_1(L),$$

, знайти такий ненульовий вектор $x \in L$ довжини $\lambda_1(L)$.

Графічний приклад розв'язку задачі SVP зображено на наступному рисунку зеленим кольором.

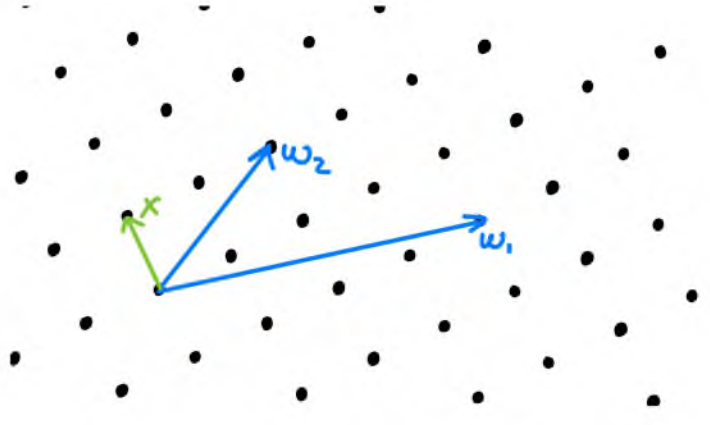

Рис. 1.2: Двовимірна решітка із базисними векторами ω_1, ω_2 та найкоротшим вектором x

Означення 1.4. *[1] Маючи решітку L у n-вимірному дійсному просторі та $x \in \mathbb{R}^n, x \notin L$, проблему пошуку найближчого вектору (Closest Vector Problem, CVP) можна описати наступним чином:*

- *знайти такий вектор* $y \in L$, *щоб*

$$\|x - y\| \leq \|x - z\|$$

для всіх $z \in L$.

- CVP_γ: *знайти такий* y, *щоб*

$$\|x - y\| \leq \gamma \cdot \|x - z\|$$

для всіх $z \in L$ *та малої константи* γ.

Графічний приклад знаходження розв'язку задачі CVP зображений на наступному рисунку зеленим кольором.

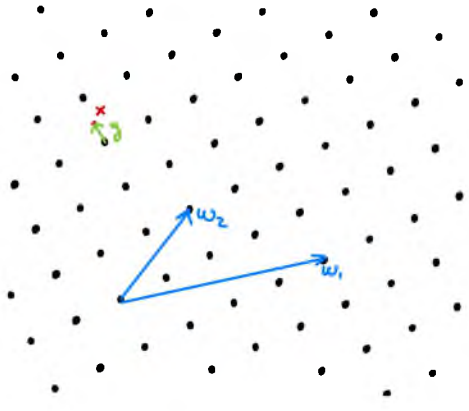

Рис. 1.3: Двовимірна решітка із базисними векторами ω_1, ω_2, точкою x, яка не належить решітці та найкоротшим вектором y до неї

Означення 1.5. *[8] Проблема пошуку найменшого базису (Smallest Basis Problem, SBP) – маючи базис* B *решітки* L *треба знайти менший базис* B' *для цієї самої решітки, у якому добуток його довжин його елементів буде найменшим.*

Наведені задачі мають експоненційну складність. Наразі не існує алгоритма, за яким можливо було б знайти розв'язки за поліноміальний час. Найшвидші поліноміальні алгоритми досягають експоненційних множників і базуються на алгоритмі LLL [1]. Цей алгоритм використовується для знаходження аппроксимованого розв'язку задач пошуку найкоротшого вектору та найменшого базису. Для знаходження наближеного розв'зяку задачі пошуку найближчого вектору використовується підхід Бабаї [1] з використанням змінених базисів.

У загальному випадку, задачі SVP, CVP та SBP розглядають як NP-складні[9].

1.1 Алгоритм Бабаї

Алгоритм Бабаї [7] вирішує задачу пошуку найближчого вектору (CVP) з наближенням $\gamma = 2^{(n-2)/2}$ за експоненційним часом.

Нехай $b_1, b_2, \ldots, b_m$ буде базисом решітки $L \subset \mathbb{R}^n$ та нехай $x \in \mathbb{R}^n$ буде довільним вектором, відстань до якого необхідно знайти. Для даного алгоритму, базисні вектори мають бути ортогональними. У випадку коли вони не є такими, доречним буде застосувати алгоритм LLL [1], який здійснює зміну базису до більш ортогонального. Задачу пошуку найближчого вектору розв'язує наступний алгоритм [2]:

1. Визначається рівняння

   $$x = t_1 b_1 + t_2 b_2 + \ldots + t_n b_n,$$

   у якому коефіцієнти $t_1, t_2, \ldots, t_n \in \mathbb{R}$;

2. Знаходиться розв'язок рівнняння та призначається $a_i = \lfloor t_i \rceil$ для $i = 1, 2, \ldots, n$;

3. Знаходиться вектор y у решітці L, наближений до вектору x:

   $$y = a_1 b_1 + a_2 b_2 + \ldots + a_n b_n.$$

У цьому розділі було розглянуто визначення решітки, наведені складні задачі на них, а саме: задача пошуку найкоротшого вектору, задача пошуку найближчого вектору та задача пошуку найменшого базису. Також було наведено алгоритм Бабаї із пошуку найкоротшого вектору.

Розділ 2

Криптосистема Голдвассер-Голдріха-Халеві

У цьому розділі ми наведемо опис криптосистеми з публічним ключом Голдвассер-Голдріха-Халеві, яка в своїй основі має складні задачі на решітках. Для кращого розуміння, як працює криптосистема буде використаний процес обміну інформацією між Алісою та Бобом [2].

Аліса обирає набір лінійно незалежних майже ортогональних між собою векторів

$$v_1, v_2, \ldots, v_n \in \mathbb{Z}^n.$$

Цей найбір векторів V вважається "хорошим" базисом, який лежить в основі решітки L та є приватним ключом Аліси. Наступним чином, генерується матриця U з цілими коефіцієнтами та $det(U) = \pm 1$. Генерування цієї матриці випадковим чином необхідно для знаходження набору векторів, який буде "поганим"базисом - публічним ключом. Одним із способів отримання матриці U є множення великої кількості випадково обраних елементарних матриць.

$$W = UV$$

Отже, ряд векторів $w_1, w_2, \ldots, w_n$ є новим базисом решітки L та є публічним ключом Аліси.

До свого повідомлення m, яке також має векторну форму та може мати вигляд бінарного вектору, Боб додає малий вектор збурення r, який є також ефімерним ключом. Наприклад, координати вектору r можуть бути випадково обрані між δ

та $-\delta$, де δ сталий публічний параметр. Далі відбувається процес шифрування:

$$e = mW + r = \sum_{i=1}^{m} m_i w_i + r,$$

де e - шифротекст, та $e \notin L$, але максимально наближений до точки $mW \in L$.

Процес дешифрування відбувається наступним чином. Аліса застосовує алгоритм Бабаї з "хорошим" базисом $v_1, v_2, \ldots, v_n$, щоб знайти вектор у решітці L, який буде найближчим до вектору шифротексту e. Враховуючи те, що вона використовує "хороший" (а отже й ортогональний) базис та вектор збурення r є малим, вектор решітки, який знаходить Аліса, являє собою mW. Помножуючи його на W^{-1}, вона знаходить оригінальне, дешифроване повідомлення від Боба m.

Розділ 3

Схема розподілу секрету

Схема розподілення секрету [3] є фундаментальним криптографічним примітивом що допускає розподілення секрету між множиною учасників, при цьому відновлення секрету можливе тільки при авторизації всіх або певної частини учасників (порогу учасників). Також необхідною умовою схеми розподілення секрету є неможливість окремих учасників, або груп учасників, кількість яких менша за поріг, відновити секрет.

Схеми розподілення секрету широко поширені в криптографії і використовуються для зберігання дуже чутливої інформації, зокрема для стійких до витоків компіляторів схем.

3.1 Загальна постановка задачі розподілу секрету

Спочатку дамо визначення k-монотонної структури доступу, потім визначимо функцію розподілу доступу, і нарешті визначимо схему розподілення секрету.

Означення 3.1.1 (**k-Монотонна схема доступу**). *[10] Схема доступу A є монотонною, якщо для будь-якої множини $S \in A$ будь-яка надмножина S також є в A. Ми будемо називати таку схему доступу k-монотонною, якщо для будь-якої множини $S \in A$, буде виконуватись $|S| \geq k$.*

Означення 3.1.2 (**Функція розподілення доступу**). *[10] Нехай $[n] = 1, 2, \ldots, n$ буде множиною ідентичностей n сторін. Нехай M буде областю секретів. Функція розподілення доступу $Share$ - це рандомізоване відображення з M на $S_1 \times S_2 \times \ldots \times S_n$, де S_i є областю поширень сторони з ідентичністю i. Для*

множини $T \subseteq [n]$ ми визначимо $Share(m)_T$ як обмеження для $Share(m)$ для її T записів.

Означення 3.1.3 ($(A, n, \varepsilon_c, \varepsilon_s)$-Схема розподілення секрету). *Нехай M буде скінченою множиною секретів, де $|M| \geq 2$. Нехай $[n] = 1, 2, \ldots, n$ буде множиною ідентичностей для n сторін. Функція поширення $Share$ із областю секретів M являє собою $(A, n, \varepsilon_c, \varepsilon_s)$-схему розподілення секрету відносно монотонної схеми доступу A, якщо виконуються наступні дві вимоги:*

- ***Коректність:*** *Секрет може бути відновленим будь-якою множиною сторін, які є частиною схеми доступу A. Тобто, для будь-якого набору $T \in A$ існує детермінована функція відновлення $Rec : \otimes_{i \in T} S_i \to M$ така, що кожне $m \in M$,*

$$Pr[Rec(Share(m)_T) = m] = 1 - \varepsilon_c$$

де ймовірність перевищує випадковість функції $Share$.

- ***Статистична конфідеційність:*** *Будь-яке об'єднання сторін, які не є частиною схеми доступу, не повинно мати майже жодної інформації про основний секрет. Тобто, для будь-якої неавторизованої множини $U \subseteq [n]$ такої щоб $U \notin A$, а також для кожної пари секретів $m_0, m_1 \in M$, для кожного обчислювально необмеженого розрізнювача D зі значенням $\{0, 1\}$, має місце наступне:*

$$|Pr[D(Share(m_0)_U) = 1] - Pr[D(Share(m_1)_U) = 1]| \leq \varepsilon_s$$

Визначимо швидкість схеми розподілення секретами як

$$lim_{|m| \to \infty} \frac{|m|}{max_{i \in [n]} |Share(m)_i|}.$$

Означення 3.1.4 (Порогова схема розподілення секрету). *Визначимо t-порогову схему як $(t, n, \varepsilon_c, \varepsilon_s)$-схему розподілення секрету.*

Узагальнюючи, схема розподілення секрету для певної схеми доступу та осіб складається з функцій $Share$, яка розподіляє секрет між учасниками схеми доступу, та Rec (Recombine), яка відновлює секрет для певної множини учасників,

якщо їх кількості достатньо для відновлення секрету. Поріг схеми розподілення секрету (t, n) визначає, що секрет може бути відтворений t кількістю учасників з загальної кількості n.

Також, схем розподілу секрету вважається безпечною, якщо жоден нескінченно потужний нападник не може нічого дізнатися про основний секрет, не маючи доступу до часток кваліфіковаої множинию. Насправді, такі схеми вважаються інформаційно-теоретично захищенними, але оскільки більшість схем обміну секретами в літературі є інформаційно-теоретично захищенними, ми просто називатимемо такі схеми безпечними.

3.2 Застосування криптосистеми Голдвассер-Голдріха-Халеві до схеми розподілу секрету

У даному розділу ми продемонструємо можливість зберігання та відтворення секрету використовуючи криптосистему GGH, яка була описана в Розділі 2. Наведена схема буде n-пороговою, тобто (n, n), а отже відновлення секрету буде можливим лише при умові наявності всіх n сторін.

Кількість базисних векторів решітки напряму залежить від кількості учасників нашої схеми. Тому, якщо кількість учасників буде дорівнювати n, то наступні лінійно незалежні майже ортогональні вектори будуть формувати нашу решітку: $v_1, v_2, \ldots, v_n$. Окремо треба зазначити, що це "хороший" базис, а отже вважається приватним ключем. Позначимо умовну решітку як L.

Далі випадковим чином генерується матриця з цілими коефіцієнтами U та $det(U) = \pm 1$. І знаходиться "поганий" базис:

$$W = UV.$$

Нагадуємо, що "поганий" базис являється публічним ключем.

Секрет, який має бути розподіленим поміж сторонами, позначимо як S. Секрет також має векторний вигляд. Шифруємо його наступним чином:

$$S_{enc} = SW + r = \sum_{i=1}^{S} S_i w_i + r,$$

де r – малий вектор збурення, який є також ефімерним ключем.

Кожній стороні схеми видається комбінація (v_i, S_{enc}). Коли всі учасники схеми збирають свої комбінації, ми отримуємо повний "хороший" базис, тоді секрет S можна відновити з допомогою алгоритму Бабаї.

Знаходимо вектор у решітці L, який буде найближчим до вектору S_{enc}. Враховуючи те, що ми маємо "хороший" базис та публічний вектор збурення r є малим, вектор решітки, який ми знаходимо, являє собою SW. Помножуючи його на W^{-1}, ми відновлюємо оригінальний секрет S.

Також можна сформулювати наступну теорему.

Теорема 3.2.1. *Схема розподілу секрету на основі криптосистеми Голдвассер-Голдріха-Халеві є коректною та статистично конфіденційною.*

Доведення. Розглянута схема є (n, n) пороговою, кожен учасник котрої має пару (v_i, S_{enc}), де v_i – частка лінійно незалежного ортогонального базису (приватного ключа) V, а S_{enc} – зашифрований секрет.

Схема розподілення секрету є коректною, оскільки

$$Pr[Rec(Share(S)_T) = m] = 1,$$

тобто секрет відновлюється з ймовірністю 1 тоді і тільки тоді, коли наявний повний "хороший" базис, а це можливо тоді і тільки тоді, коли множина сторін n є повною, тобто присутні всі n сторін.

Схема є також статистично конфіденційною, бо у випадку наявності пари секретів m_0 та m_1, $n-1$ кількість учасників не матимуть можливість зрозуміти, до якого секрету відносяться наявні в них ключі, оскільки частинами ключів є зашифруванні секрети m_0 та m_1 за допомогою криптосистеми Голдвассер-Голдріха-Халеві. □

Як приклад розглянемо схему з трьома учасниками. Маємо наступні три базисні вектора, що формують решітку L:

$$v_1 = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, v_2 = \begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix}, v_3 = \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}.$$

Вони є "хорошим" базисом V - приватним ключом. Далі генеруємо матрицю U, у якої $det(U) = \pm 1$:

$$U = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix}$$

Тепер знаходимо "поганий" базис $W = UV$:

$$W = UV = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & -2 \\ 2 & -2 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 3 & 3 \\ 3 & 0 & 3 \\ 1 & -1 & -4 \end{pmatrix},$$

який є публічним ключем.

Маємо секрет $S = (240, 80, 1991)$ та вектор збурення $r = (1, 0, -1)$. Шифруємо наш секрет:

$$S_{enc} = SW + r = (240, 80, 1991) \begin{pmatrix} 6 & 3 & 3 \\ 3 & 0 & 3 \\ 1 & -1 & -4 \end{pmatrix} + (1, 0, -1) =$$

$$= (3671, -1271, -7004).$$

Кожнен із трьох учасників схеми отримує свою пару (v_i, S_{enc}):

- перший учасник отримує $\left(\begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}, (3671, -1271, -7004) \right)$;
- другий учасник отримує $\left(\begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix}, (3671, -1271, -7004) \right)$;
- третій учасник отримує $\left(\begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}, (3671, -1271, -7004) \right)$.

Для відновлення секрету, застосуємо алгоритм Бабаї. Ми шукатимемо найближчий вектор решітки із базисними векторами V до S_{enc}. Запишемо S_{enc} у

вигляді $S_{enc} = t_1 v_1 + t_2 v_2 + t_3 v_3$:

$$\begin{pmatrix} 3671 \\ -1271 \\ -7004 \end{pmatrix} = t_1 \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} + t_2 \begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix} + t_3 \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix},$$

розв'язуючи це рівняння отримуємо

$$t_1 = -1431 = a_1, t_2 = 2231 = a_2, t_3 = 320 = a_3.$$

Далі обчислюємо $y = a_1 v_1 + a_2 v_2 + a_3 v_3$ та отримуємо:

$$y = -1431 \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} + 2231 \begin{pmatrix} 2 \\ 1 \\ -2 \end{pmatrix} + 320 \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix} = \begin{pmatrix} 3671 \\ -1271 \\ -7004 \end{pmatrix},$$

y буде найближчим вектором до S_{enc}. Тепер, щоб відновити секрет S, треба обчислити yW^{-1}:

$$S = yW^{-1} = (3671, -1271, -7004) \cdot \frac{1}{18} \begin{pmatrix} 1 & 3 & 3 \\ 5 & -9 & -3 \\ -1 & 3 & -3 \end{pmatrix} = \begin{pmatrix} 240 \\ 80 \\ 1991 \end{pmatrix}$$

Отриманий дешифрований результат збігається з первинним секретом.

Висновки

Кваліфікаційну роботу присвячено розробці схеми розподілення секрету, що базується на криптосистемі Голдвассер-Голдріха-Халеві (GGH).

У розділі 1 були розглянуті теоретичні відомості про складні задачі на решітках, а саме: пошук найкоротшого вектору (SVP), пошук найближчого вектору (CVP) та пошук найменшого базису (SBP). Ці задачі лежать в основі багатьох криптосистем на решітках, бо їх обчислення займає експоненційний час. Також було наведено алгоритм Бабаї для пошуку найближчого вектору.

Далі, у розділі 2, було розглянуто криптосистему GGH.

У розділі 3 було побудовано нову (n, n)-порогову схему розподілу секрету, що має в своїй основі криптосистему GGH. Доведено, що запропонована схема розподілу секрету є коректною та статистично конфіденційною. Наведено приклад розподілу секрету для трьох сторін за запропонованою схемою. Результати прикладу відображають правильну роботу запропонованого методу розподілу секрету.

Дана робота є логічним продовженням курсової роботи та має потенціал для подальших досліджень – а саме, можливість побудови (t, n) порогової схеми розподілу секрету на основі GGH криптосистеми.

Список літератури

[1] Smart N. P. *Cryptography Made Simple* — Springer International Publishing Switzerland — 481 p. — 2016.

[2] Hoffstein J., Pipher J., Silverman J.H. *An Introduction to Mathematical Cryptography* — Springer Science+Business Media, LLC — 523p. — 2016.

[3] Shamir A. *How to share a secret* — Communications of the Association for Computing Machinery. — V.22, №11. p.612-613 — 1995.

[4] Binu V.P., Sreekumar A. *Simple and Efficient Secret Sharing Schemes for Sharing Data and Image* — International Journal of Computer Science and Information Technologies — Vol. 6(1), p. 404-409 — 2015.

[5] Ravi P., Howe J., Chattopadhyay A., Bhasin S. *-Lattice-Based Key Sharing Schemes: A Survey* — ACM Computing Surveys, Volume 54, Issue 1 — Article №9, p. 1-39 — 2021.

[6] Alford W.R., Granville A., Pomerance C. *There are infinitely many Carmichael numbers* — Ann. of Math.(2), — 139(3):703-722, — 1994.

[7] Babai L., *On Lovász' lattice reduction and the nearest lattice point problem* — Combinatorica, 6:1-13, — 10.1007/BF02579403 — 1986.

[8] Goldreich O., Goldwasser S., Halevi S. *Public-key cryptosystems from lattice reduction problems* — Proceedings of 17th Annual International Cryptology Conference, — Santa Barbara, California, USA. — pp. 112-131, — 1997.

[9] Nguyen P. *Cryptoanalysis of the Goldreich–Goldwasser–Halevi Cryptosystem from Crypto'97* — Advances in Cryptology, — 1999.

[10] Srinvasan A., Vasudevan P. N. *Leakage Resilient Secret Sharing and Applications* — Advances in Cryptology, — CRYPTO 2019, pp. 480-509 — 2019.