УДК 004.056.55

ОБЧИСЛЮВАЛЬНА СКЛАДНІСТЬ ОСНОВНИХ ЗАДАЧ НА АЛГЕБРАЇЧНИХ РЕШІТКАХ

М.Ф. БОНДАРЕНКО, Л.В. МАКУТОНІНА

Наводяться огляд та результати порівняльного аналізу основних обчислювальних задач, що використовують алгебраїчні решітки.

Ключові слова: алгебраїчні решітки, обчислювальна складність, базис решітки, найкоротший вектор у решітці.

ВСТУП

Криптографічні перетворення на алгебраїчних решітках належать до досить нової галузі в криптографії, але є найперспективнішою галуззю, що швидко та потужно розвивається. Першою потенціальною стійкою криптосистемою з відкритим ключем на алгебраїчних решітках вважається криптосистема NTRU, яка була вперше представлена в 1996 році, та яка була запатентована 24 липня 2000 року. З тих пір було запропоновано безліч криптосистем та криптопримітивів, що використовують алгебраїчні решітки [1–6], в тому числі, і на ідентифікаційних даних [7–10].

Одним із найважливіших питань, для криптосистем на алгебраїчних решітках, є визначення стійкості задачі, що лежить в основі конкретної криптографічної схеми. Тому, метою даної статті є визначення та порівняльний аналіз стійкості обчислювальних задач на решітках.

1. ОСНОВНІ ВІДОМОСТІ, ЩО СТОСУЮТЬСЯ АЛГЕБРАЇЧНИХ РЕШІТОК

Решітка – це множина n-лінійно незалежних векторів, тобто решітка з розмірністю n – це набір лінійних комбінацій b_i з цілими коефіцієнтами a_i, тоді решітку L можна подати так:

$$L=\{a_1b_1+\ldots+a_nb_n \mid a_i\in Z^k\}, \qquad (1)$$

де k – ранг решітки. Базисом решітки називають набір лінійно незалежних k-векторів виду: $b_1,\ldots,b_n$, де $b_i\in R^n$. Параметр n є параметром безпеки, і, зазвичай, інші параметри залежать від нього.

Розглянемо основні положення, які є необхідними для подальшого аналізу криптографічної стійкості задач на алгебраїчних решітках.

Довжина вектора x у решітці вимірюється його нормою $\|x\|$. Найчастіше для решіток використовується норма Евкліда, що визначається як:

$$\|x\|=\sqrt{\sum_{i=1}^{n}x_i^2}. \qquad (2)$$

Мінімальна відстань $\lambda_1(L)$ решітки L визначається, як $\min_{x\neq y}\|x-y\|$, де x,y – елементи решітки L. Мінімальна відстань еквівалентна довжині найкоротшого ненульового елемента, тобто $\lambda_1(L)=\min_{x\in L,x\neq 0}\|x\|$. Для даного набору точок S на решітці, $\|S\|$ визначається, як $\max\|s\|$, де максимум береться над усіма елементами $s\in S$.

Нехай q – просте. Тоді, нехай $A\in Z_q^{n\times m}$, тобто A – матриця елементи якої належать до Z_p. Найчастіше, зустрічаються такі два види алгебраїчних решіток [11]:

$$L(A,q)=\{y\in Z^m : y=A^T s \bmod q, \text{ для деякого } s\in Z^n\}; \qquad (3)$$

$$L^{\perp}(A,q)=\{e\in Z^m : Ae=0 \bmod q\}. \qquad (4)$$

Тут, A^T означає транспоновану матрицю A, що породжує решітку $L(A,q)$, A – матриця перевірки парності для решітки $L^{\perp}(A,q)$. Решітку, визначену над Z_q, називають модулярною решіткою.

2. КЛАСИФІКАЦІЯ ТА ЗАГАЛЬНИЙ ОПИС ОСНОВНИХ ОБЧИСЛЮВАЛЬНИХ ЗАДАЧ, ЯКІ ЗАСНОВАНІ НА АЛГЕБРАЇЧНИХ РЕШІТКАХ

Однією із статей, в якій вперше було надано оцінку та вимоги до обчислювальних задач на решітках, є стаття Айтаі [12]. Так, у 1996 році Айтаі сформулював три базові задачі на алгебраїчних решітках, які лягли в основу більшості подальших задач, на алгебраїчних решітках:

1. Знайти довжину найкоротшого ненульового вектора в n-вимірній решітці, з точністю до поліноміального фактору.

2. Знайти найкоротший ненульовий вектор v у n-вимірній решітці L, для якої найкоротший вектор v є унікальним, тобто, будь-який інший вектор, з довжиною не більш за $n^c\|v\|$, є паралельним до вектора v, де, c – достатньо велика абсолютна константа.

3. Знайти базис $b_1,\ldots,b_n$, в n-вимірній решітці L, з довжиною, що визначена, як $\max_{i=1}^{n}\|b_i\|$, і, що є найменшою з можливих, з точністю до поліноміального фактору.

Основні обчислювальні задачі на алгебраїчних решітках можна умовно класифікувати так:

1. Задачі, що засновані на пошуку найкоротшого вектора. До цього класу відносяться задачі, що базуються на пошуку першого послідовного мінімуму в решітці L, що дорівнює довжині найкоротшого ненульового вектора решітки (мінімальній відстані між двома точками в решітці L), тобто, $\lambda_1(L) = \min\{\|x\| \mid x \in L, x \neq 0\}$. Першою очевидною задачею в теорії решіток є пошук ненульового вектора, який би досягав цього мінімуму. Зазначимо також, що такий вектор ніколи не є унікальним, оскільки $\|-x\| = \|x\|$, для усіх векторів решітки $x \in L$ (в решітці існують інші точки з цією ж нормою).

2. Задачі, що засновані на пошуку найближчого вектора. До цього класу відносяться задачі, які базуються на пошуку, для даної точки $t \in R^n$, найближчої точки в решітці L, причому, припускається, що $t \notin L$. Така точка може бути не унікальною, але в багатьох випадках вона є такою.

3. Задачі, що засновані на пошуку найкоротшого набору векторів. До цього класу відносяться задачі, що базуються на прямому зведенні задачі про знаходження найкоротшого вектора в решітці L, тобто поданні, для якого перший послідовний мінімум подається як пряме узагальнення повної послідовності послідовних мінімумів. Такі мінімуми визначаються так: $\lambda_i(L) = \min\{\max\{\|x_1\|,\ldots,\|x_i\|\} \mid x_1,\ldots,x_i \in L,$ лінійно незалежні$\}$.

4. Задачі, що засновані на модулярних решітках. Решітка $L \subset Z^m$ називається модулярною за модулем q, або q-нарною, якщо $qZ^m \subset L$. Зазвичай, використовуються решітки, для яких $q << \mathrm{vol}(L)$, де $\mathrm{vol}(L)$ – потужність решітки L. У даній статті розглядатимуться модулярні решітки виду $L_{A,q} = \{x \in Z^m \mid Ax \equiv 0 (\mathrm{mod}\, q)\}$, де A – матриця розмірністю $n \times m$, з цілими коефіцієнтами взятими за модулем q.

5. Задачі, що засновані на ідеальних решітках. Для даного типу задач $R = Z[x]/\langle f \rangle$ – кільце цілочисельних поліномів за модулем деякого нормованого полінома f ступеня n. Оскільки R ізоморфно до Z^n, тоді адитивна група та ідеали в кільці R, що визначені підгрупами, відповідають решітці. Решітку такого виду називають ідеальною решіткою по відношенню до f.

6. Задачі, що засновані на пошуку радіусу покриття. Радіусом покриття для даної, можливо нескінченої, множини точок P решітки L у Евклідовому просторі, є найменше число r таке, що сфера з радіусом r навколо всіх точок P покриває весь простір.

3. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА ПОШУКУ НАЙКОРОТШОГО ВЕКТОРА

Задача пошуку найкоротшого вектора в решітці (SVP- задача) є класичною задачею в теорії чисел. Найкращі алгоритми, які існують на сьогодні, розв'язують дану задачу за експоненціальний час. Айтай у роботі [12] показав, що SVP-задача є NP-повною задачею.

1) SVP-задача (The Shortest Vector Problem)

Вхідні дані: Базис решітки L.

Завдання: Знайти $y \in L$, такий, що $\|y\| = \lambda_1(L)$.

2) SVP γ-задача (The Approximate Shortest Vector Problem)

Вхідні дані: Базис решітки L, апроксимаційний фактор $\gamma \geq 1$.

Завдання: Знайти $y \in L$, такий, що $0 < \|y\| \leq \gamma\lambda_1(L)$.

Відомо, що SVP γ-задача є NP- складною [13], для $\gamma = 2^{\log^{1/2-\varepsilon}(n)} \approx \sqrt{n}$.

Для двох наведених вище задач значення $\lambda_1(L)$ не є відомим, але, замість цього значення може бути використано значення $\mathrm{vol}(L)$, що є відомим, задачу такого типу називають Ермітовим варіантом апроксимації SVP- задачі (див. наступну задачу).

3) HSVP γ-задача (The Hermite Shortest Vector Problem)

Вхідні дані: Базис решітки L, апроксимаційний фактор $\gamma > 0$.

Завдання: Знайти $y \in L$, такий, що $0 < \|y\| \leq \gamma \mathrm{vol}(L)^{1/n}$.

У роботі [13] показано, що алгоритм Ленстри-Ленстри-Ловаса (далі – LLL) [14] розв'язує останню задачу за поліноміальний час для $\gamma = (\sqrt{4/3} + \varepsilon)^{(n-1)/2}$, на практиці це значення приблизно дорівнює $\gamma = 1{,}02^n$.

4) DSVP- задача (The Decision Shortest Vector Problem)

Вхідні дані: Базис решітки L, радіус $r > 0$.

Завдання: Визначити, чи існує $y \in L$, такий, що $0 < \|y\| \leq r$.

Наступна задача основується на припущенні, про можливість знаходження першого послідовного мінімуму, без знання найкоротшого ненульового вектора в решітці.

5) SLP γ-задача (The Approximate Shortest Length Problem)

Вхідні дані: Базис решітки L, апроксимаційний фактор $\gamma > 1$.

Завдання: Знайти λ, таке, що

$$\lambda_1(L) \leq \lambda \leq \gamma\lambda_1(L),$$

де $\lambda_1(L)$ – перший послідовний мінімум.

Говорять, що $L' \subset L$, з рангом $n' < n$, таким, що $\mathrm{vol}(L')^{1/n'}$, є істотно меншою за решітку з $\mathrm{vol}(L)^{1/n'}$. Інакше кажучи, існують вектори решітки L, такі, що є коротшими ніж очікувалося у випадковій решітці. Такий розрив між першими двома послідовними мінімумами отримав назву наступної апроксимації SVP-задачі.

6) USVP γ-задача (The Unique Shortest Vector Problem)

Вхідні дані: Базис решітки L, фактор лакуни $\gamma \geq 1$.

Завдання: Знайти, якщо такий існує, унікальний ненульовий вектор $y \in L$, такий, що для будь-якого $v \in L$ з $\|v\| \leq \gamma\|y\|$ є кратним y.

7) GapSVP γ-задача (The Gap Shortest Vector Problem)

Вхідні дані: Базис решітки L, раціональне число $r>0$, апроксимаційний фактор $\gamma>1$.

Завдання: Якщо $\lambda_1(L)\le r$, повернути відповідь «Так»; якщо $\lambda_1(L)>\gamma r$, повернути «Ні».

Хот у роботі [15] показав, що GapSVP γ - задача є NP-складною для деякого константного значення γ.

Хот і Вішной у роботі [16] сформулювали визначення ще двох апроксимацій SVP- задачі, які залежать від l_p - норми, що наведені нижче. Також, у роботі [16] було показано, що наступні дві задачі є NP-складними для деякого $p\ge 1$. Для будь-якого $p\ge 1$ визначена l_p - норма вектора $x=(x_1,x_2,\ldots,x_n)\in R^n$ так: $\|x\|_p:=(\sum_{i=1}^n|x_i|^p)^{1/p}$.

8) USVP p - задача (Unique Shortest Vector Problem in l_p norm)

Вхідні дані: Базис $\{b_1,\ldots,b_n\}\in Z^n$ решітки L, раціональне число $r>0$.

Завдання: Якщо в решітці L існує рівно два ненульових вектора $(v,-v)$ з нормою l_p меншою, ніж r, повернути відповідь «Так»; якщо в решітці L не існує ненульовий вектор з нормою l_p меншою, ніж r, повернути відповідь «Ні».

9) PSVP p - задача (Unique Shortest Vector Problem in l_p norm)

Вхідні дані: Базис $\{b_1,\ldots,b_n\}\in Z^n$ – набір лінійно-незалежних ненульових векторів, з довжиною щонайменше за одиницю з нормою l_p.

Завдання: Якщо в решітці L існує ненульовий вектор з довжиною меншою, ніж ς, повернути відповідь «Так»; якщо в решітці L усі ненульові вектори мають довжину меншу, ніж ς, повернути відповідь «Ні».

4. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА ПОШУКУ НАЙБЛИЖЧОГО ВЕКТОРА

Задача пошуку найближчого вектора в решітці (CVP- задача) є однією з найголовніших задач в теорії алгебраїчних решіток. Найкращі алгоритми, які існують на сьогодні, розв'язують дану задачу за експоненціальний час, але існує алгоритм, який запропонував Бабаі [17], що вирішує апроксимацію даної задачі за поліноміальний час. Даний алгоритм використовує метод форсування нуля (обнуління) з послідовним усуненням перешкод (Zero Forcing with Successive Interference Cancellation) [18].

1) CVP- задача (The Closest Vector Problem)

Вхідні дані: Базис решітки L, цільовий вектор $t\in R^n$.

Завдання: Знайти ненульовий вектор $y\in L$, такий, що $\|t-y\|=n(t,L)$.

2) CVP γ - задача (The Approximate Closest Vector Problem)

Вхідні дані: Базис решітки L, цільовий вектор $t\in R^n$, апроксимаційний фактор $\gamma\ge 1$.

Завдання: Знайти ненульовий вектор $y\in L$, такий, що $\|t-y\|=\gamma n(t,L)$.

Санджив Арора та ін. [19] показали, що CVP γ - задача є NP- складною для деякого константного значення γ, та, імовірно, що дана задача є NP- складною для $\gamma=2^{\log^{1-\varepsilon}n}\approx n$. Алгоритм Бабаі вирішує CVP γ - задачу за поліноміальний час для $\gamma=2(\sqrt{4/3})^n$ [13,17].

3) DCVP- задача (The Decision Closest Vector Problem)

Вхідні дані: Базис решітки L, цільовий вектор $t\in R^n$, радіус $r>0$.

Завдання: Визначити, чи існує $y\in L$, такий, що $\|y-t\|\le r$.

Існують криптосистеми, які нібито засновані на CVP- задачі, але, при цьому, не відомо чи є відстань між решіткою і цільовою точкою обмеженою. Тому, зазвичай, використовують таку апроксимацію CVP- задачі, що є простішою.

4) BDD α -задача (Bounded Distance Decoding)

Вхідні дані: Базис решітки L, параметр відстані $\alpha>0$, цільовий вектор $t\in R^n$, такий, що $n(t,L)<\alpha\lambda_1(L)$.

Завдання: Знайти таке $y\in L$, що $n(y,t)=n(L,t)$.

Стійкість BDD α - задачі залежить від значення α, і BDD α - задача є NP- складною для $\alpha>1/2\sqrt{2}$ [20].

5) GapCVP γ - задача (The Gap Closest Vector Problem)

Вхідні дані: Базис решітки L, цільовий вектор $t\in R^n$, дійсні числа $\gamma,r>0$.

Завдання: Якщо $\|y-t\|\le r$, повернути відповідь «Так»; якщо $\|y-t\|>\gamma r$, повернути «Ні».

5. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА ПОШУКУ НАЙКОРОТШОГО НАБОРУ ВЕКТОРІВ

Вперше задачу, що заснована на пошуку базису мінімальної довжини в алгебраїчній решітці, запропонував Айтаі у 1996 році [12], яка в даній статті наведена під назвою SBP.

1) SBP- задача (The Shortest Basis Problem)

Вхідні дані: Решітка L, n -вимірна, з довжиною, визначеною, як $\max_{i=1}^n\|b_i\|$.

Завдання: Знайти найменший базис даної решітки $\{b_1,\ldots,b_n\}$, з точністю до поліноміального фактору.

В роботі [12] Айтаі довів, що $\max_{i=1}^n\|b_i\|\le n^c\,\mathrm{bl}(L)$, для деякої абсолютної константи c, з імовірністю $1-2^{-\sigma}$.

2) SBP γ - задача (The Approximate Shortest Basis Problem)

Вхідні дані: Базис $\{a_1,\ldots,a_n\}$ решітки L, апроксимаційний фактор $\gamma\ge 1$.

Завдання: Знайти такий базис $\{b_1,\ldots,b_n\}$ решітки L, що $\max_i\|b_i\|\le\gamma\min\{max_i\|a_i\|\,|\{a_1,\ldots,a_n\}\in L\}$.

3) SMP γ - задача (The Successive Minima Problem)

Вхідні дані: Базис $\{b_1,\ldots,b_n\}$ решітки L.

Завдання: Знайти лінійно незалежний набір $\{y_1,\ldots,y_n\}$ такий, що $\|y_i\|=\lambda_i(L)$, для $i=1,\ldots,n$.

Також існує SMP γ - задача з апроксимаційним фактором $\gamma > 1$, що визначається аналогічно з SMP- задачею, з точністю до γ.

4) SIVP- задача (The Shortest Independent Vector Problem)

Вхідні дані: Базис $\{b_1,...,b_n\}$ решітки L.

Завдання: Знайти лінійно незалежний набір $\{y_1,...,y_n\}$, такий, що $\max_i \|y_i\| \le \lambda_n(L)$.

5) SIVP γ - задача (The Approximate Shortest Independent Vector Problem)

Вхідні дані: Базис $\{b_1,...,b_n\}$ решітки L, апроксимаційний фактор $\gamma \ge 1$.

Завдання: Знайти лінійно незалежний набір $\{y_1,...,y_n\}$, такий, що $\max_i \|y_i\| \le \gamma\lambda_n(L)$.

Блумер і Сейферт у роботі [21] показали, що SIVP γ - задача є NP-складною для $\gamma = n^{1/\log\log n}$.

6) GapSIVP γ - задача (The Gap Shortest Independent Vector Problem)

Вхідні дані: Решітка L, m -вимірна, з базисом $\{b_1,...,b_n\} \in Z^n$ таким, що $m \ge n$, в Евклідовому просторі, апроксимаційний фактор $\gamma \ge 1$, пара (B,d), де B – ранг, d – раціональне число.

Завдання: Якщо $\lambda_n(B) \le d$, повернути відповідь «Так»; якщо $\lambda_n(B) > \gamma(n)\cdot d$, повернути відповідь «Ні».

Далі розглянемо загальний випадок SIVP- задачі, тобто дещо спрощений випадок SIVP- задачі, який було сформульовано в роботі [22].

7) GIVP $_{\gamma}^{\phi}$ - задача (Generalized Independent Vectors Problem)

Вхідні дані: Базис $B = \{b_1,...,b_n\}$ n -вимірної решітки L.

Завдання: Знайти такий набір лінійно незалежних векторів $S = \{s_1,...,s_n\} \subset L(B)$, що $\|S\| \le \gamma(n)\cdot\phi(B)$.

Зазвичай ϕ означає деяку довільну функцію решітки. Якщо обрати $\phi = \lambda_n$, тоді в результаті отримаємо) SIVP- задачу. В роботі [22] ϕ означає параметр згладжування, який пов'язаний з розподілом Гауса.

6. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА МОДУЛЯРНИХ РЕШІТКАХ

Вперше задачу вирішення малих цілих (SIS- задача) було запропоновано в [22].

1) SIS- задача (Small Integer Solutions Problem)

Вхідні дані: Решітка $L_{A,q}$, модуль q, матриця $A \pmod q$, $v < q$.

Завдання: Знайти таке $y \in Z^m$, що $Ay \equiv 0 \pmod q$ і $\|y\| \le v$.

2) ISIS- задача (Inhomogeneous Small Integer Solutions Problem)

Вхідні дані: Решітка $L_{A,q}$, $x \in Z^n$, модуль q, матриця $A \pmod q$, $v < q$.

Завдання: Знайти таке $y \in Z^m$, що $Ay \equiv x \pmod q$ і $\|y\| \le v$.

Задача навчання з помилками (LWE-задача) була запропонована Регевом у [23]. Нехай q – модуль. Для $s \in Z_q^n$ і ймовірнісного розподілу χ над Z_q нехай $A_{s,\chi}$ – ймовірнісний розподіл над $Z_q^n \times Z_q$ з вибіркою такого виду: $a \in Z_q^n$ обирається рівномірно, $e \in Z_q$ обирається відповідно до χ, далі повертається $(a, \langle a,s\rangle + e) \pmod q$.

3) LWE- задача (Learning With Errors Problem)

Вхідні дані: Решітка $L_{A,q}$, n, розподіл χ (бажано дискретний Гауса), модуль q, будь-яке число незалежних вибірок з $A_{s,\chi}$.

Завдання: Знайти s.

4) DLWE- задача (Decision Learning With Errors Problem)

Вхідні дані: Решітка $L_{A,q}$, n, розподіл χ (бажано дискретний Гауса), модуль q, будь-яке число незалежних вибірок з $A_{s,\chi}$.

Завдання: Якщо були обрані елементи вибірки з $A_{s,\chi}$, повернути відповідь «Так»; якщо були обрані елементи з нормального розподілу повернути відповідь «Ні».

7. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА ІДЕАЛЬНИХ РЕШІТКАХ

Перші дві задачі, які наведені нижче, були запропоновані Любашевським і Міссіансіо в роботі [24]. На сьогодні не відомо, чи є наступні задачі NP- складними. Для наступних двох задач, визначимо: для будь-якого ідеалу I над $Z[x]/\langle f\rangle$, де f – це незвідний цілочисельний поліном ступеня n, $\lambda_i^p(I)$ дорівнює $\lambda_i^p(L(I))$.

1) IdealSPP γ - задача (Approximate Shortest Polynomial Problem)

Вхідні дані: Ідеал I решітки L в $Z[x]/\langle f\rangle$.

Завдання: Знайти поліном $g \in I \setminus \{0\}$, такий, що $\|g\|_f \le \gamma\lambda_1^{\infty}(I)$.

Для того щоб сформулювати наступну задачу, дамо визначення фактору розширення (Expansion Factor), який відноситься до властивостей f: $EF(f,k) = \max_{g \in Z[x], \deg(g) \le k(\deg(f)-1)} \|g\|_f / \|g\|_{\infty}$.

2) IdealISPP γ - задача (Approximate Incremental Shortest Polynomial Problem)

Вхідні дані: Ідеал I решітки L в $Z[x]/\langle f\rangle$, поліном $g \in I$, такий, що $\|g\|_f > \gamma\lambda_1^{\infty}(I)$.

Завдання: Знайти $h \in I$, таке, що $\|h\|_f \ne 0$.

Задача IdealSPP γ зводиться за поліноміальний час до IdealISPP γ - задачі [24].

Штеле та ін. у роботі [5] сформулювали дві задачі на решітках IdealSIS$_{q,m}^{f}$ і IdealLWE$_{q,m}^{\chi}$, що засновані на задачах найгіршого випадку IdealSIS і IdealLWE, запропонованих в [22,25]. Спочатку сформулюємо найгірший випадок задачі IdealSIS.

3) IdealSIS $_{q,m,\beta}^{f,p}$ - задача (Ideal Small Integer Solution Problem), найгірший випадок.

Вхідні дані: Поліноми m і n, $g_1,...,g_m$ обрані рівномірно і випадково з $Z_q[x]/\langle f\rangle$.

Завдання: Знайти $e_1,...,e_m$ в $Z[x]$, такі, що $\sum_{i \prec m} e_i g_i = 0 \pmod q$ і $\|e\|_p \le \beta$, де e – це вектор, обчислений шляхом конкатенації всіх коефіцієнтів e_i's.

4) IdealSIS $_{q,m}^{f}$ - задача (Approximate Ideal Small Integer Solution Problem)

Вхідні дані: Решітка L, m-вимірна.

Завдання: Знайти невеликий ненульовий елемент $M^{\perp}(g)=\{b\in(Z[x]/f)^m,\langle b,g\rangle=0 \bmod q\}$ з $Z[x]/\langle f\rangle$, де $g=(g_1,\ldots,g_m)$.

5) IdealLWE$^{\chi}_{q,m}$ - задача (Ideal Learning With Errors Problem).

Вхідні дані: Параметр n, матриця $G\in Z^{m(n)\times n}_{q(n)}$ обрана рівномірно і випадково, і $Gs+e\in(R/[1,q(n)])^n$, де $s\in Z^n_{q(n)}$ обране рівномірно і випадково, координати $e\in(R/q(n))^{m(n)}$ незалежно обраного з $\chi(n)$.

Завдання: Знайти s.

8. ЗАДАЧІ, ЯКІ ЗАСНОВАНІ НА РАДІУСІ ПОКРИТТЯ

Одед Регев та ін. у роботах [26,27] сформулювали та надали аналіз стійкості задачі покриття радіусу в алгебраїчній решітці (CRP- задача).

1) CRP- задача (Covering Radius Problem)

Вхідні дані: Решітка L, n-вимірна, з множиною точок P.

Завдання: Знайти раціональне число r, таке, щоб сфера з радіусом r навколо всіх точок P покрила весь простір.

Для того щоб сформулювати наступну задачу, дамо визначення радіусу покриття. Радіус покриття $\rho(B)$ решітки

$$L=\{x\in\text{span}(L):\forall y\in L,\langle x,y\rangle\in Z\}$$

з максимальною відстанню $dist(x,\rho(B))$, визначається так: $\rho(B)=\max\limits_{x\in span(B)}\{dist(x,\rho(B))\}$. Наступна задача також визначена для лінійних кодів [27].

2) GapCRPγ-задача (The Gap Covering Radius Problem)

Вхідні дані: Решітка L, m-вимірна, з базисом $\{b_1,\ldots,b_n\}\in Z^n$ таким, що $m\geq n$, в Евклідовому просторі, апроксимаційний фактор $\gamma\geq 1$, пара (B,r), де B – ранг, r – раціональне число.

Завдання: Якщо $\rho(B)\leq r$, повернути відповідь «Так»; якщо $\rho(B)>\gamma(n)\cdot r$, повернути відповідь «Ні».

В роботі [27] була проаналізована складність даної задачі і доказано, що задача радіуса покриття для n-вимірної решітки з апроксимаційним фактором $\gamma(n)$ задовольняє такі властивості:

– для будь-якої константи $\gamma(n)>1$ задача може бути ймовірносно розв'язана за час $2^{O(n)}$;

– для $\gamma(n)=\sqrt{n}$, задача є NP∩coNP- стійкою;

– для $\gamma(n)=2^{\Omega(n\log\log n/\log n)}$, задача може бути розв'язана за випадковий поліноміальний час;

– для $\gamma(n)=2^{\Omega(n(\log\log n)^2/\log n)}$, задача може бути розв'язана за детермінований поліноміальний час.

Пізніше, у роботі [26] було доведено, що для будь-якого достатньо великого $p\leq\infty$, існує константа $c_p>1$, така, що CRP^p - задача є Π_2 - стійкою, відносно апроксимаційного фактору c_p.

Наступна задача наведена в роботі [22]. Зазвичай параметр ϕ, який раніше було описано в задачі GIVP$^{\phi}_{\gamma}$, для наступної задачі означає радіус покриття решітки.

3) GDD$^{\phi}_{\gamma}$- задача (Guaranteed Distance Decoding Problem)

Вхідні дані: Базис $B=\{b_1,\ldots,b_n\}$ n-вимірної решітки L, цільова точка t.

Завдання: Знайти точку $x\in L(B)$ в решітці L, таку, що $\text{dist}(t,x)\leq\gamma(n)\cdot\phi(B)$.

Зазначимо, що для будь-якого базису B у решітці і цільової точки $t\in R^n$ завжди існує точка в решітці з відстанню $\phi(B)$ від t, де $\phi(B)$ – це радіус покриття.

9. ОБЧИСЛЮВАЛЬНА СКЛАДНІСТЬ ОСНОВНИХ ЗАДАЧ НА РЕШІТКАХ

Результати порівняльного аналізу складності основних обчислювальних задач на алгебраїчних решітках були зведені до табл. 1.

Задачі, що засновані на ідеальних решітках, а також HSVPγ, DSVP, DCVP, GapCVPγ, SBPγ, SMPγ, SIVP, GapSIVPγ, GIVP$^{\phi}_{\gamma}$, SIS, ISIS, LWE, DLWE, CRP і GDD$^{\phi}_{\gamma}$ не були включені до табл. 1, оскільки на сьогодні не відомо, чи є вони NP- складними, та поки що не надано будь-яких оцінок їхньої стійкості.

ВИСНОВОК

У роботі наведено огляд досягнень галузі криптографії, що динамічно розвивається, а саме алгебраїчних решіток. Робота містить необхідні базові визначення, опис основних задач теорії решіток, а також наведені існуючі на сьогодні результати аналізу стійкості основних задач на решітках.

Найважливішими із задач у теорії решіток є SVP і CVP, саме ці задачі породжують майже всі існуючі апроксимації задач на алгебраїчних решітках. Якщо проаналізувати існуючі результати стійкості даних задач, можна сказати, що на сьогодні відкрито питання доказу стійкості більшості з цих задач. Але, тим не менш, існуючі криптосистеми на алгебраїчних решітках мають відносно високу швидкодію, і є стійкими до квантових атак, тому, дане питання є перспективним напрямом вивчення і досліджень у криптографії та прикладній криптології.

Література

[1] *Daniele Micciancio.* Improving lattice based cryptosystems using the Hermite normal form / In Joseph H. Silverman, edit. – Proceedings of the 1st international conference held in Providence. – Lecture Notes in Computer Science «Cryptography and lattices». – Vol.2146. – Springer. – 2001. – P.126–145.

[2] *Oded Regev.* New lattice-based cryptographic constructions / Journal of the ACM. – Vol.51. – 2004. – P.899–942.

Таблиця 1

Результати порівняльного аналізу складності основних задач на решітках

№	Задача	Обчислювальна складність	Результати, стосовно розв'язання даної задачі
1.	SVP	NP- повна задача [12]	Усі існуючі алгоритми вирішують не менш ніж за експоненціальний час
2.	SVP γ	NP- складна [13], для деякого $\gamma = 2^{\log^{1/2-\epsilon}(n)} \approx \sqrt{n}$ [13]	Не існує поліноміальних алгоритмів, для l_p - норми, з константним фактором, та над $\mathrm{NP} \not\subseteq \mathrm{RTIME}(2^{poly(\log n)})$, для деякого $2^{(\log n)^{1/2-\epsilon}}$ [15]
3.	HSVP γ	-	LLL- алгоритм [14] вирішує за поліноміальний час, для $\gamma = (\sqrt{4/3}+\varepsilon)^{(n-1)/2}$ [13]
4.	SLP γ	Вважається, що є NP- складною в найгіршому випадку[12]	-
5.	GapSVP γ	NP-складна для деякого константного значення γ [15]	-
6.	USVP p	NP-складна для деякого $p \geq 1$ з l_p - нормою [16]	-
7.	PSVP p	NP-складна для деякого $p \geq 1$ з l_p - нормою [16]	-
8.	CVP	CVP = CVP_1 є NP- складною [29]	Усі існуючі алгоритми вирішують не менш ніж за експоненціальний час
9.	CVP γ	NP- складна для деякого константного значення γ, та, імовірно, є NP- складною для $\gamma = 2^{\log^{1-\epsilon} n} \approx n$ [19]	Алгоритм Бабаї вирішує за поліноміальний час для $\gamma = 2(\sqrt{4/3})^n$ [13,17]
10.	BDD α	Залежить від α [20], є NP- складною для $\alpha > 1/2\sqrt{2}$	-
11.	SBP	Вважається, що є NP- складною в найгіршому випадку[12]	-
12.	SIVP γ	NP- складна [21], для деякого $\gamma = n^{1/\log\log n}$	-
13.	GapCRP γ	Для деякого $\gamma(n) = \sqrt{n}$, є NP∩coNP- складною[27]	Для будь-якої константи $\gamma(n) > 1$ може бути ймовірнісно вирішена за час $2^{O(n)}$

[3] *O. Regev.* Lattice-based cryptography / In Advances in cryptology (CRYPTO). – 2006. – P.131–141.

[4] *Akinori Kawachi, Keisuke Tanaka, Keita Xagawa.* Multi-bit cryptosystems based on lattice problems / In Tatsuaki Okamoto, Xiaoyun Wang edit. – Lecture Notes in Computer Science «Public key cryptography—PKC 2007». – Vol.4450. – Springer. – 2007. – P.315–329.

[5] *Damien Stehlй, Ron Steinfeld, Keisuke Tanaka, Keita Xagawa. Efficient* Public Key Encryption Based on Ideal Lattices / In Mitsuru Matsui, edit. – Lecture Notes in Computer Science «Advances in Cryptology». – Vol.5912. – Springer. – 2009. – P.617–635.

[6] *Yi Ding, Lei Fan.* Efficient Password-Based Authenticated Key Exchange from Lattices / In Yuping Wang, Yiu-ming Cheung, Ping Guo, Yingbin Wei, edit. – Seventh International Conference on Computational Intelligence and Security. – 2011. – P.934–938.

[7] *Shweta Agrawal, Dan Boneh, Xavier Boyen.* Efficient Lattice (H)IBE in the Standard Model / Lecture Notes in Computer Science «Advances in Cryptology – EUROCRYPT 2010». – Vol.6110. – Springer-Verlag. – 2010. – P.553–572.

[8] *Jin Wang, Jingguo Bi.* Lattice-based Identity-Based Broadcast Encryption Scheme [Електронний ресурс] / Cryptology ePrint Archive. – Report 2010/288.– Режим доступу: http://eprint.iacr.org/2010/288.

[9] *Shweta Agrawal, Xavier Boyen.* Identity-based encryption from lattices in the standard model. [Електронний ресурс] / Manuscript. – Режим доступу: http://www.cs.stanford.edu/~xb/ab09/.

[10] *Amit Sahai, Brent Waters.* Fuzzy identity-based encryption / In Ronald Cramer, edit. – Lecture Notes in Computer Science «Advances in Cryptology - EUROCRYPT 2005». – Vol.3494. – Springer. – 2005. – P. 457–473.

[11] *Sanjit Chatterjee, Palash Sarkar.* Identity-Based Encryption / Springer Science + Business Media, LLC. – 2011. – P.125–135.

[12] *Miklys Ajtai.* Generating Hard Instances of Lattice Problems (Extended Abstract) / In Gary L. Miller, edit. – Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing. – STOC. – Vol.28. – 1996. – P. 99–108.

[13] *Thijs Laarhoven, Joop van de Pol, Benne de Weger.* Solving Hard Lattice Problems and the Security of Lattice-Based Cryptosystems [Електронний ресурс] / Cryptology ePrint Archive. – Report 2012/533.– Режим доступу: http://eprint.iacr.org/2012/533.

[14] *A.K. Lenstra, H.W. Lenstra, L. Lovasz.* Factoring polynomials with rational coefficients / Mathematische Annalen. – Vol.261(4). – Springer-Verlag. – 1982. – P. 515–534.

[15] *Subhash Khot.* Hardness of approximating the shortest vector problem in lattices / Journal of the ACM. – Vol.52(5). – 2005. – P. 789–808.

[16] *Subhash Khot, Nisheeth K. Vishnoi.* Hardness of Lattice Problems in lp Norm [Електронний ресурс] / Microsoft Research. – Режим доступу: http://research.microsoft.com/en-us/um/people/nvishno/webpapers/kv03svpusvp.pdf.

[17] *Lőszly Babai.* On Lovбsz' lattice reduction and the nearest lattice point problem / Combinatorica. – Vol.6(1). – Springer. – 1986. – P. 1–13.

[18] *H. Yao, G. W. Wornell.* Lattice-reduction-aided detectors for MIMO communication systems / IEEE Global Telecommunications Conference (GLOBECOM 2002). – 2002. – P. 17–21.

[19] *Sanjeev Arora, Lőszly Babai, Jacques Stern, Z. Sweedyk.* The Hardness of Approximate Optimia in Lattices, Codes, and Systems of Linear Equations / Proc. of the 34th Annual Symposium on Foundations of Computer Science IEEE. – Computer Society Press. – 1993. – P. 724–733.

[20] *Y.K. Liu, V. Lyubashevsky, D. Micciancio.* On bounded distance decoding for general lattices / In Josep Diaz, Klaus Jansen, Jose D.P. Rolim, Uri Zwick, edit. – Lecture Notes in Computer Science «Approximation, Randomization, and Combinatorial Optimization, Algorithms and Techniques». – Vol.4110. – Springer. – 2006. – P. 450–461.

[21] *J. Blomer, J.P. Seifert.* On the complexity of computing short linearly independent vectors and short bases in a lattice / Proc. of the 31st annual ACM symposium on Theory of Computing (STOC '99). – 1999. – P. 711–720.

[22] *Daniele Micciancio, Oded Regev.* Worst-Case To Average-Case Reductions Based On Gaussian Measures / SIAM Journal on Computing. – Vol.37(1). – 2007. – P. 267–302.

[23] *Oded Regev.* The Learning with Errors Problem (Invited Survey) / Proc. of the 25th Annual IEEE Conference on Computational Complexity (CCC 2010). – IEEE Computer Society. – 2010. – P. 191–204.

[24] *Vadim Lyubashevsky, Daniele Micciancio.* Generalized compact knapsacks are collision resistant / In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, Ingo Wegener, edit. – Lecture Notes in Computer Science. – Part II. – Vol.4052. – Springer. – 2006. – P. 144–155.

[25] *Craig Gentry, Chris Peikert, Vinod Vaikuntanathan.* Trapdoors for hard lattices and new cryptographic constructions / In Richard E. Ladner, Cynthia Dwork edit. – STOC. – ACM. – 2008. – P. 197–206.

[26] *Ishay Haviv, Oded Regev.* Hardness of the Covering Radius Problem on Lattices. Proc. of the 21st Annual IEEE Conference on Computational Complexity (CCC 2006). – IEEE Computer Society. – 2006. – P. 145–158.

[27] *Venkatesan Guruswami, Daniele Micciancio, Oded Regev.* The Complexity of the Covering Radius Problem on Lattices and Codes / Proc. of the 19th Annual IEEE Conference on Computational Complexity (CCC 2004). – IEEE Computer Society. – 2004. – P.161-173.

[28] J.H. van de Pol. Lattice-based cryptography. – Eindhoven University of Technology. – Eindhoven. – 2011. – 106p. [Докторська дисертація].

[29] P van Emde Boas. Another NP-complete partition problem and the complexity of computing short vectors in a lattice / Technical Report. – Vol.81-04. – Mathematisch Instituut. – 1981.

Надійшла до редколегії 13.03.2013

Бондаренко Михайло Федорович, член-кореспондент НАН України, Лауреат державної премії України, доктор технічних наук, професор, ректор Харківського національного університету радіоелектроніки.

Макутоніна Лідія Вікторівна, аспірант кафедри БІТ ХНУРЕ. Наукові інтереси: асиметричні системи шифрування, криптографічні системи та протоколи, що засновані на ідентифікаторах та алгебраїчних решітках.

УДК 004.056.55

Вычислительная сложность основных задач на алгебраических решетках / М.Ф. Бондаренко, Л.В. Макутонина // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 258–264.

Приводятся обзор и результаты сравнительного анализа основных вычислительных задач, использующих алгебраические решетки..

Ключевые слова: алгебраическая решетка, вычислительная сложность, базис решетки, кратчайший вектор в решетке.

Табл.: 1. Библиогр.: 29 назв.

UDK 004.056.55

Computational complexity of algebraic lattice basic problems / M.F. Bondarenko, L.V. Makutonina // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 258–264.

A review and comparative analysis of basic computational problems using algebraic lattices are provided.

Keywords: algebraic lattice, computational complexity, lattice base, shortest vector in the lattice.

Tab.: 1. Ref.: 29 items.