УДК 004.056.55

АНАЛІЗ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ НА ІДЕНТИФІКАТОРАХ, ЩО ВИКОРИСТОВУЮТЬ АЛГЕБРАЇЧНІ РЕШІТКИ

І.Д. ГОРБЕНКО, Л.В. МАКУТОНІНА

Наводяться огляд та результати порівняльного аналізу основних алгоритмів криптографічних перетворень на ідентифікаторах, що використовують алгебраїчні решітки. Обґрунтовуються вибір параметрів, з точки зору забезпечення необхідного рівня стійкості. Наводяться умови та доказ безпеки для задачі навчання в моделі випадкового оракула з помилками.

Ключові слова: криптографічні системи на ідентифікаторах, алгебраїчні решітки, алгоритм зашифрування, алгоритм розшифрування, ідентифікатор користувача, прообраз вибірки, функція з секретом.

ВСТУП

Впровадження та використання існуючої інфраструктури відкритих ключів на сертифікатах, виявило ряд недоліків і проблемних питань, до яких можна віднести складність побудови, складність використання для кінцевого користувача і вартість. Альтернативою таким системам є криптосистеми з відкритим ключем на ідентифікаторах. Існує два перспективних напрями побудови криптографічних систем на ідентифікаторах (Identity-Based Encryption – IBE) – з використанням білінійних спаровувань на еліптичних кривих (ЕК) та з використанням решіток [6, 7, 18]. Існує також і третій підхід, який полягає в використанні елементарного теоретично-числового методу, запропонованого Коксом, Боне, Жентрі і Гамбургом [1, 2].

Метою даної статті є порівняльний аналіз основних схем на ідентифікаторах, що використовують алгебраїчні решітки та обґрунтування вибору кращої з них.

До недавнього часу майже всі IBE-конструкції були засновані на білінійних спарюваннях точок еліптичних кривих, але з появою роботи Джентрі, Вейкунтанатана і Пейкерта [3] особливий інтерес спостерігається з боку побудови криптографічних схем на ідентифікаторах, що використовують задачі на решітках. У даній статті описано і проаналізовано нові підходи побудови IBE-конструкцій, що використовують алгебраїчні решітки, та даються відповідні оцінки.

1. СХЕМА ДЖЕНТРИ, ВЕЙКУНТАНАТАНА І ПЕЙКЕРТА

Джентрі, Вейкунтанатана і Пейкерта показали [3], що можливо побудувати набір функцій з секретом з праобразу вибірки, що засновані на складності вирішення задачі про решітки. Запропонована схема використовує допоміжний алгоритм SampleD, та складається з трьох основних кроків:

1. Генерація функцій з секретом. Для будь-якого q (поліноміально обмеженого параметром безпеки n) та будь-якого $m \geq 5n\log_2 q$ існує імовірнісний алгоритм з поліноміальним часом виконання, який за вхідні значення приймає: 1^n виходів матриці $\mathbf{A} \in Z_q^{n\times m}$; повно ранговий набір $\mathbf{S} \subset \Lambda^{\perp}(\mathbf{A},q)$, з розподіленням A статистично близьким до рівномірного над $Z_q^{n\times m}$; $\|\mathbf{S}\| \leq L = m^{2,5}$. Переважна ймовірність належить $\mathbf{A}$ з рангом n.

2. Визначається функція $f_{\mathbf{A}}(\mathbf{e}) = \mathbf{Ae} \bmod qZ_q^{n\times m}$, ранг $R_n = Z_q^n$ та домен $D_n = \{\mathbf{e} \in Z^m : \|\mathbf{e}\| \leq s\sqrt{m}\}$. Використовуючи алгоритм SampleD може бути обране $D_{Z^m,s}$ розподілення по D_n, зі стандартним базисом для Z^m.

3. Застосовується інверсний алгоритм функції з секретом SampleISIS, з вхідними значеннями $(\mathbf{A},\mathbf{S},s,\mathbf{u})$, який обирає зі $f_{\mathbf{A}}^{-1}(\mathbf{u})$. Спочатку використовуються лінійні алгебраїчні функції для обчислення $\mathbf{t} \in Z^m$, такого, що $\mathbf{At} = \mathbf{u} \bmod q$. Після цього використовується алгоритм SampleD зі функцією з секретом $\mathbf{S}$ та вибірка $\mathbf{v}$ з розподілу $D_{\Lambda^{\perp},s,-\mathbf{t}}$, вихідним значенням алгоритму є $\mathbf{e} = \mathbf{t} + \mathbf{v}$.

Допоміжний алгоритм SampleD для кожного базису решітки $\mathbf{B} \in Z^{n\times k}$, кожного ідеалу $s \geq \|\mathbf{B}\| \cdot w(\sqrt{\log n})$ та кожного $\mathbf{c} \in IR^n$, виробляє вихідну послідовність SampleD$(\mathbf{B},s,\mathbf{c})$, з розподілом, в межах статистично незначної відстані $D_{L(\mathbf{B}),s,\mathbf{c}}$. Алгоритм виконується в поліноміальному часі з розміром вхідної послідовності n.

В основі схеми Джентрі, Вейкунтанатана і Пейкерта [3] лежить ідея обчислення підпису з геш-значення прообразу в заданому діапазоні. В IBE-схемах ключ розшифрування для заданого ідентифікатора можна розглядати як підпис уповноваженого на генерацію для даного ідентифікатора. Так, шляхом обчислення геш-значення ідентифікатора в діапазоні, через генерацію одного із прообразів, можливо обчислити ключ розшифрування. Хоча схема є концептуально простою, існують труднощі, які полягають в зіставленні випадкового оракула з ідентифікатором у заданому діапазоні.

Нехай n визначає параметр безпеки, та нехай $q = q(n)$ – просте, $m = m(n)$ – позитивне ціле число (аналогічно $O(n\log n)$), розмірність решітки.

1. Встановлення параметрів (Set-Up)

За допомогою алгоритму генерації функції з секретом, генерується матриця $\mathbf{A} \in Z_q^{n\times m}$ та функція з секретом $\mathbf{S} \subseteq \Lambda^{\perp}(\mathbf{A},q)$: для будь-якого $\mathbf{u} \in Z_q^n$

застосовується функція з секретом **S**, обирається $\mathbf{e} \in Z_q^m$ з набору всіх прообразів **u** над f.

Відкритими параметрами є: матриця **A**. Майстер ключ: **S**.

2. Вироблення секретного ключа користувача (Key-Gen).

Секретний ключ користувача генерується для відповідного ідентифікатора, який потім зберігається. На подальші запити ключа користувачу надається раніше генерований секретний ключ.

Під час генерації секретного ключа для ідентифікатора $id \in \{0,1\}^*$ використовується функція гешування $H:\{0,1\}^* \to Z_q^n$, що побудована для моделі з випадковим оракулом. Для даного id, нехай $\mathbf{u} = H(id)$, використовуючи майстер ключ **S** обчислюється **e** – прообраз **u** над f.

Секретний ключем для даного id є: **e**.

Нехай χ – розподіл в Z_q і χ^m – m-кратний добуток розподілу в Z_q^m. Розподіл χ має параметр r, що має бути обраним таким, щоб забезпечити складність розкриття, що дорівнює складності вирішення задачі «навчання з помилками» (learning with errors – LWE) над решітками [22].

3. Алгоритм зашифрування (Encrypt)

Зашифрування біта повідомлення b для ідентифікатора id виконується наступним чином:

a) нехай $\mathbf{u} = H(id) \in Z_q^n$;

b) рівномірно обирається **s** з Z_q^n;

c) встановлюється $\mathbf{p} = \mathbf{A}^{\mathrm{T}}\mathbf{s} + \mathbf{x}$, де **x** обирається з Z_q^m відповідно до розподілу χ^m;

d) обчислюється $c = \mathbf{u}^{\mathrm{T}}\mathbf{s} + x + b\lfloor q/2 \rfloor$, де x обирається з Z_q відповідно до χ.

Зашифрованим текстом є пара $(c, \mathbf{p})$.

4. Алгоритм розшифрування (Decrypt)

Розшифрування криптограми біта повідомлення $(c, \mathbf{p})$ для ідентифікатора id, за наявності отриманого від центру секретного ключа **e**, виконується наступним чином:

a) обчислюється $b' = c - \mathbf{e}^{\mathrm{T}}\mathbf{p} \in Z_q$;

b) якщо $b' \notin [0, \lfloor q/2 \rfloor) \bmod q$, вихідним значенням є 1; інакше – 0.

В алгоритмі зашифрування обирається вектор $\mathbf{p} = \mathbf{A}^{\mathrm{T}}\mathbf{s} + \mathbf{x}$ для рівномірно випадкового **s** і **x** обраного з χ^m. Даний вектор по суті є LWE-вектором. Вектор **u** є прикладом ще одного LWE-вектора для генерації $p = \mathbf{u}^{\mathrm{T}}\mathbf{s} + x$, де x обирається з χ. Значення p використовується як маска повідомлення b (перетворення $b \cdot \lfloor q/2 \rfloor$). Доки **u** є рівномірним для криптоаналітика криптограма також є рівномірною (в припущенні, що LWE є важко розв'язуваною). З цієї причини, ця схема має властивість анонімності зашифрованого тексту відносно до особи, яка його зашифрувала.

Більш формально, можна показати, що для правильно зашифрованого повідомлення, розшифрування може бути успішним з переважною ймовірністю, і, що схема CPA-безпечна і анонімна за умови, якщо LWE-задача з відповідно заданими параметрами є важко розв'язуваною.

Зашифрування здійснюється по одному біту за раз. В результаті, розмір зашифрованого тексту є досить великим. Певною мірою ця проблема може бути вирішена наступним чином. Припустимо, що повідомлення є k-бітним рядком. Ідентифікатори відображаються як H до k елементів $\mathbf{u}_1,\ldots,\mathbf{u}_k \in Z_q^n$, де $\mathbf{u}_i$ використовується для зашифрування i-го біта повідомлення. Випадкове **s** використовується для всіх бітів, і тому вектор $\mathbf{p} = \mathbf{A}^{\mathrm{T}}\mathbf{s} + \mathbf{x}$ залишається однаковим для кожного зашифрування. Відмітимо, що k-елементів з Z_q^m будуть частиною секретного ключа.

2. СХЕМА АГРАВАЛ, БОНЕ І БОЄНА

Схема запропонована Агравал, Боне і Боєном є різновидом схем ієрархічного шифрування на ідентифікаторах (HIBE). У попередній роботі Агравал, Боне і Боєна [4], ідентифікатор відображається в елемент **u** і, для обчислення прообразу, використовується функція з секретом **S**. Матриця **A** попередньо обчислюється і не залежить від ідентифікатора. На вищому рівні ця схема є подібною до класичної IBE-схеми Боне-Франкліна [5], де ідентифікатори відображаються в точки на ЕК і ключем розшифрування є результат s-разового скалярного множення цих точок.

Альтернативний підходом до побудови IBE-шифрування на решітках є заміна ролі діапазону точки на відображення матриці. У звичайній HIBE-схемі діапазон точки **u** є фіксованим і не залежить від ідентифікатора. Матриця **A** змінюється в $[\mathbf{A}_0 \,|\, \mathbf{A}_1 + H(id)\mathbf{B}]$, де $\mathbf{A}_0, \mathbf{A}_1, \mathbf{B}$ відносяться до відкритих параметрів, а $H: Z_q^n \to Z_q^{n \times n}$ є відкритою функцією, що відображає ідентифікатор (що вважається елементом Z_q^n) в матрицю. Функція H відображає Z_q^n до $Z_q^{n \times n}$, і задовольняє властивості «повно рангової різниці»: для будь-яких двох різних $\mathbf{u}, \mathbf{v} \in Z_q^n$, матриця $H(\mathbf{u}) - H(\mathbf{v})$ є повно ранговою.

Розглянемо матрицю $\mathbf{F} = [\mathbf{A}, \mathbf{AR} + \mathbf{B}]$, де $\mathbf{A}, \mathbf{B} \in Z_q^{n \times m}$ та $\mathbf{R} \in \{-1,1\}^{m \times m}$. Використовуються два метода відбору прообразів SampleLeft та SampleRight [6]. Метод SampleLeft працює зі скороченим базисом для **A**, і базується на узагальненому прообразі вибірки. Метод SampleRight базується на техніці делегації решітки. В реальних IBE-схемах використовується тільки метод SampleLeft, а метод SampleRight використовується тільки при моделюванні параметра безпеки.

Схема Агравал, Боне і Боєна [7] представлена наступним чином:

1. Встановлення параметрів (Set-Up)

Для даних n,q використовується метод генерації функції з секретом [8] для генерації матриці $\mathbf{A}_0 \in Z_q^{n \times m}$ та скорочений базис $\mathbf{S}_0$ для $\Lambda^{\perp}(\mathbf{A}_0)$. Обираються дві рівномірні випадкові матриці $\mathbf{A}_1, \mathbf{B} \in Z_q^{n \times m}$. Обирається рівномірно та випадково $\mathbf{u} \in Z_q^n$. Ідентифікатори вважаються елементами Z_q^n, для будь-якого ідентифікатора id, нехай:

$$\mathbf{F}_{id} = [\mathbf{A}_0, \mathbf{A}_1 + H(id)\mathbf{B}].$$

Відкритими параметрами є: $\mathbf{A}_0, \mathbf{A}_1, \mathbf{B}, \mathbf{u}$. Майстер ключ: $\mathbf{S}_0$.

2. Вироблення секретного ключа користувача (Key-Gen).

Нехай *id* – ідентифікатор, використаємо скорочений базис $\mathbf{S}_0 \subseteq \Lambda^{\perp}(\mathbf{A}_0)$ для обчислення прообразу $\mathbf{e}_{id} \in Z_q^{2m}$ над $\mathbf{u}$ для $\mathbf{F}_{id}$. Остання дія є алгоритмом SampleLeft, який узагальнює метод відбору прообразу. Тоді $\mathbf{F}_{id}\mathbf{e}_{id} = \mathbf{u}$.

Секретний ключем для даного *id* є: прообраз $\mathbf{e}_{id}$.

3. Алгоритм зашифрування (Encrypt).

Зашифрування біта повідомлення *b* для ідентифікатора *id* виконується наступним чином:

a) рівномірно випадково обирається $s \in Z_q^n$;

b) рівномірно випадково обирається матриця $\mathbf{R} \in \{-1,1\}^{m \times m}$;

c) обирається елемент шуму $x \in Z_q$ відповідно до розподілу $\bar{\Psi}_\alpha$;

d) обирається елемент шуму $y \in Z_q^m$ відповідно до розподілу $\bar{\Psi}_\alpha^m$;

e) встановлюється $\mathbf{z} = \mathbf{R}^{\mathrm{T}}\mathbf{y}$;

f) обчислюється $c_0 = \mathbf{u}^{\mathrm{T}}\mathbf{s} + x + b\lfloor q/2 \rfloor$;

g) обчислюється $\mathbf{c}_i = \mathbf{F}_{id}{}^{\mathrm{T}}\mathbf{s} + \begin{bmatrix} y \\ z \end{bmatrix} \in Z_q^{2m}$.

Зашифрованим текстом є пара $(c_0, \mathbf{c}_1)$.

4. Алгоритм розшифрування (Decrypt).

Розшифрування криптограми біта повідомлення $(c_0, \mathbf{c}_1)$ для ідентифікатора *id*, за наявності отриманого від центру секретного ключа $\mathbf{e}_{id}$ для даного ідентифікатора, виконується наступним чином:

a) обчислюється $w = c_0 - \mathbf{e}_{id}^{\mathrm{T}}\mathbf{c}_1 \in Z_q$;

b) як цілі числа порівнюються w і $\lfloor q/2 \rfloor$, якщо $|w - \lfloor q/2 \rfloor| < \lfloor q/4 \rfloor|$, вихідним значенням є 1; інакше – 0.

Відмітимо, що на повідомлення накладається маска аналогічно з попередньою схемою. Стандартний аналіз показує, що розшифрування є успішним з більш ніж переважною ймовірністю. Матриця **R** грає ключову роль в забезпеченні захищеності схеми. Безпека даної схеми доведена в селективно-ідентифікаційній моделі. Мета криптоаналітика – створення ідентифікатора користувача id^*, який потім встановлюється в IBE-схемі замість *id*.

3. АНАЛІЗ БЕЗПЕКИ СХЕМ, ЩО ЗАСНОВАНІ НА LWE-ЗАДАЧАХ

У реальній IBE-схемі, функція з секретом для матриці $\mathbf{A}_0$ є відомою. З іншого боку, для схем, заснованих на LWE-задачах, функція з секретом для матриці $\mathbf{A}_0$ є не відомою. Але центр повинен бути в змозі відповісти на запити вироблення ключа. Це є можливим за умови створення функції з секретом для матриці **B** і використання алгоритму SampleRight наступним чином.

Припустимо, що метою криптоаналітика є створення ідентифікатора користувача id^*. Центр встановлює IBE-схему, в звичайному порядку, генеруючи **u**. Далі центр генерує випадкову матрицю $\mathbf{A}_0 \in Z_q^{n \times m}$ і пару $(\mathbf{B}, \mathbf{T})$, використовуючи алгоритм генерації функції з секретом, де $\mathbf{B} \in Z_q^{n \times m}$ і **T** скорочений базис для решітки $\Lambda^{\perp}(\mathbf{B})$. Для генерування зашифрованого тексту необхідна випадкова матриця $\mathbf{R} \in \{-1,1\}^{m \times m}$. Так як ці параметри не залежать від запитів криптоаналітика, то вони обираються при налаштуваннях. Матриця $\mathbf{A}_1$ визначається, як:

$$\mathbf{A}_1 = \mathbf{A}_0, \mathbf{R}^* - H(id^*)\mathbf{B}.$$

Оголошуються відкриті параметри $(\mathbf{A}_0, \mathbf{A}_1, \mathbf{B}, \mathbf{u})$. При цьому центр не має функції з секретом для $\mathbf{A}_0$, але має функцію з секретом для **B**.

Припустимо, що криптоаналітик робить запит на вироблення ключа для ідентифікатора *id*. Тоді $\mathbf{F}_{id}$ формується наступним чином:

$$\mathbf{F}_{id} = [\mathbf{A}_0, \mathbf{A}_1 + H(id)\mathbf{B}] =$$
$$= [\mathbf{A}_0, \mathbf{A}_0\mathbf{R}^* + (H(id) - H(id^*))\mathbf{B}].$$

З властивості про повно рангову різницю H, витікає, що $H(id) - H(id^*)$ не сингулярне. Також, з великою ймовірністю **B** не сингулярне, і, тоді $\mathbf{B}' = (H(id) - H(id^*))\mathbf{B}$ також не сингулярне. Знання функції з секретом **T** для **B** дозволяє центру за допомогою алгоритму SampleRight обчислити прообраз **u** для $\mathbf{F}_{id}$. Причому, алгоритм SampleRight вимагає скорочений базис для **B'**, тоді, як насправді центр має скорочений базис для **B**. Таким чином, центр може відповісти на будь-які запити вироблення ключа, крім для id^*.

Розподілення $(c_0^*, \mathbf{c}_1^*)$ в реальних схемах є таким, що в LWE-випадку вхідні значення мають «реальне» розподілення. В останньому доказі безпеки, як є прийнятим, це розподілення є «випадковим», тобто, $(c_0^*, \mathbf{c}_1^*)$ обирається рівно ймовірно і випадково з $Z_q \times Z_q^{2m}$. Тоді криптоаналітик не має переваги в атаці селективної підробки ідентифікатора. Крім того, показано, що відмінності між цими двома атаками обмежені зверху перевагою рішення LWE-задачі.

4. НЕЧІТКЕ IBE-ШИФРУВАННЯ НА РЕШІТКАХ

З розвитком схеми шифрування, питання забезпечення підтримки комплексних політик доступу, стає все більш актуальним. Зокрема, стає необхідним поява систем, на основі функціонального шифрування. В даних схемах, власник секретного ключа може розшифрувати дані, та/або будь-яку частину, та/або функцію від цих даних, не просто на основі рішення одержувача (одержувачів), а на основі сформованої політики. Переваги таких схем є очевидними – доступ до зашифрованих даних виходить за рамки простого переліку, стаючи потенційно довільною функцією.

З моменту появи нечіткого шифрування на ідентифікаторах [9], з'явилися кілька систем, що вийшли за рамки традиційної «призначено отримувачу» парадигми шифрування. У рамках напрямку даних робіт [10, 11], ключ,або, в деяких варіантах, зашифрований текст, пов'язується з предикатом, скажімо, функцією f, в той же час, зашифрований текст (або ключ) пов'язаний з атрибутом, скажімо, вектором x. Розшифрування є успішним, тоді і тільки тоді, коли $f(x)=1$. Зокрема, шифрування на основі атрибутів [12-17], відноситься до випадку, коли предикат у вигляді булевої формули, з даними атрибутами, забезпечує двійкові входи. Нечітке IBE-шифрування являє собою особливий випадок, коли функція f є *k-out-of-l* пороговою функцією. У шифруванні, на основі предикатів, предикат f повинен обчислюватись без будь-яких знань про атрибути, окрім знань двійкової вихідної послідовності з $f(x)$. Однак, конструкції такого типу поки що обмежені предикатами, що задаються всередині схеми, тобто, впровадженими константами і атрибутами деякого поля.

Схема нечіткого IBE-шифрування на решітках

С. Агравал та ін. у роботі [18] запропонували таку схему. Нехай $\lambda \in Z^+$ – буде параметром безпеки. Нехай $q=q(\lambda)$ буде простим, $n=n(\lambda)$ і $m=m(\lambda)$ два позитивних цілих числа, $\sigma=\sigma(\lambda)$ і $\alpha=\alpha(\lambda)$ два позитивних параметра Гауса. Припустимо, що $\mathrm{id}\in\{0,1\}^l$, для деякого $l\in N$.

1. Встановлення параметрів (Set-Up)

Алгоритм за вхідні значення приймає параметр безпеки λ і довжину ідентифікатора l:

1. Використовується алгоритм **TrapGen**(1^λ) для вибору $2l$ рівномірних випадкових $n\times m$ матриць $A_{i,b}\in Z_q^{n\times m}$ (для усіх $i\in[l]$, $b\in\{0,1\}$) разом з повно-ранговим набором векторів $\mathbf{T}_{i,b}\subseteq\Lambda_q^{\perp}(\mathbf{A}_{i,b})$, таких, що $\|\tilde{\mathbf{T}}_{i,b}\|\le m\cdot w(\sqrt{\log m})$.

2. Обирається рівномірний і випадковий вектор $\mathbf{u}\in Z_q^n$.

Відкритими параметрами є:

$$\mathrm{PP}=(\{\mathbf{A}_{i,b}\}_{i\in[l],b\in\{0,1\}},\mathbf{u}).$$

Майстер ключ: $\mathrm{MK}=(\{\mathbf{T}_{i,b}\}_{i\in[l],b\in\{0,1\}})$.

2. Вироблення секретного ключа користувача (Key-Gen)

Алгоритм за вхідні значення приймає відкриті параметри PP, майстер ключ MK, ідентифікатор $\mathrm{id}\in\{0,1\}^l$ і поріг $k\le l$:

1. Будується l частин від $\mathbf{u}=(u_1,\ldots,u_n)\in Z_q^n$, шляхом застосування схеми розподілу секрету Шаміра незалежно для кожної координати $\mathbf{u}$. А саме, для кожного $j\in[n]$, обирається рівномірно і випадково поліном $p_j\in Z_q[x]$ ступеню $k-1$, такий, що $p_j(0)=u_j$.

Будується j - та частка вектора:

$$\hat{\mathbf{u}}_j=(\hat{u}_{j,1},\ldots,\hat{u}_{j,n})\overset{\mathrm{def}}{=}$$
$$=(p_1(j),p_2(j),\ldots,p_n(j))\in Z_q^n.$$

Забігаючи наперед (до розшифрування), відмітимо, що для всіх $J\subset[l]$, таких, що $|J|\ge k$, можна обчислити дробові коефіцієнти Лагранжа L_j, такі, що $\mathbf{u}=\sum_{j\in J}L_j\cdot\hat{\mathbf{u}}_j(\mathrm{mod}\,q)$. Тобто, ми інтерпретуємо L_j у вигляді дробі цілих чисел, яку також можна оцінити $(\mathrm{mod}\,q)$.

2. Використовуючи функцію з секретом MK і алгоритм SamplePre, знаходимо $\mathbf{e}_j\in Z^m$, таке, що $\mathbf{A}_{j,\mathrm{id}_j}\cdot\mathbf{e}_j=\hat{\mathbf{u}}_j$, для $j\in[l]$.

Секретним ключем для даного id є: $(\mathbf{e}_1,\ldots,\mathbf{e}_l)$.

3. Алгоритм зашифрування (Encrypt).

Алгоритм за вхідні значення має: відкриті параметри PP, ідентифікатор id, повідомлення $b\in\{0,1\}$:

1. Нехай $D\overset{def}{=}(l!)^2$.
2. Рівномірно та випадково обирається $\mathbf{s}\xleftarrow{R}Z_q^n$.
3. Обирається терм шуму $x\leftarrow\chi_{\{\alpha,q\}}$ і $\mathbf{x}_i\leftarrow\chi_{\{\alpha,q\}}{}^m$.
4. Встановлюється $c_0\leftarrow\mathbf{u}^{\mathrm{T}}\mathbf{s}+Dx+b\lfloor q/2\rfloor\in Z_q$.
5. Встановлюється $\mathbf{c}_i\leftarrow\mathbf{A}_{i,\mathrm{id}_i}{}^{\mathrm{T}}\mathbf{s}+D\mathbf{x}_i\in Z_q^m$ для всіх $i\in[l]$.

Зашифрованим текстом є: $\mathbf{CT}_{\mathrm{id}}:=(c_0,\{\mathbf{c}_i\}_{i\in[l]})$.

4. Алгоритм розшифрування (Decrypt)

Алгоритм на вході має відкриті параметри PP, секретний ключ $\mathrm{SK}_{\mathrm{id}}$ і зашифрований текст $\mathrm{CT}_{\mathrm{id}'}$:

1. Нехай $J\subset[l]$ позначає множину відповідних бітів для id та id′. Якщо $|J|<k$, на виході є $\perp$. В іншому випадку, можна обчислити дробові коефіцієнти Лагранжа L_j, так, що $\sum_{j\in J}L_j\mathbf{A}_j\mathbf{e}_j=\mathbf{u}(\mathrm{mod}\,q)$.

2. Обчислюється

$$r\leftarrow c_0-\textstyle\sum_{j\in J}L_j\cdot\mathbf{e}_j^{\mathrm{T}}\mathbf{c}_j(\mathrm{mod}\,q),$$

де $r\in\left[-\lfloor q/2\rfloor,\lfloor q/2\rfloor\right)\subset Z$.

3. Якщо $|r|<q/4$, вихідним значенням є 0, інакше 1.

5. АНАЛІЗ БЕЗПЕКИ, ОЦІНКА ВИБОРУ СИСТЕМНИХ ПАРАМЕТРІВ І ДОВЖИН КЛЮЧІВ ДЛЯ НЕЧІТКОГО IBE-ШИФРУВАННЯ НА РЕШІТКАХ

Аналіз безпеки нечітких IBE-схем на решітках

Вважається, що конструкція нечіткого IBE-шифрування забезпечує селективно-ідентифікаційну безпеку. При цьому, передбачається, що обраний зашифрований текст нічим не відрізняється від випадкового елемента в просторі зашифрованого тексту [19].

Твердження 1. Якщо існує PPT зловмисник A з перевагою $T>0$ в грі над селективною моделлю безпеки для нечіткої IBE-схеми з попереднього розділу, тоді існує PPT алгоритм B, який вирішує LWE-задачу з перевагою $T/(l+1)$.

Доведення твердження. LWE-задача, на прикладі, реалізується як оракул O, який може бути дійсно випадковим $O_\$$, або псевдовипадковим O_s оракулом шуму, для деякого секретного ключа $s \in Z_q^n$. Центр B використовується криптоаналітиком A для того, щоб розрізнити ці два оракула, тоді можна зімітувати алгоритм дій криптоаналітика. Нехай A повідомляє B ідентифікатор id^*, замінюючи ним дійсний id.

Центр B звертається до O, отримує $(lm+1)$ LWE вибірок, визначені, як:

$$\{(\mathbf{w}_1^1, v_1^1),(\mathbf{w}_1^2, v_1^2),\ldots,(\mathbf{w}_1^m, v_1^m)\},\ldots,$$
$$\{(\mathbf{w}_l^1, v_l^1),(\mathbf{w}_l^2, v_l^2),\ldots,(\mathbf{w}_l^m, v_l^m)\} \in \{Z_q^n \times Z_q\}^{(lm+1)}.$$

1. Встановлення параметрів. Центр B встановлює відкриті системні параметри PP, наступним чином:

a. Обирається l матриць $\mathbf{A}_{i,\mathrm{id}_i^*}$, $i \in [l]$ з LWE задачі $\{(\mathbf{w}_i^1),(\mathbf{w}_i^2),\ldots,(\mathbf{w}_i^m)\}_{i\in[l]}$. Обирається l матриць $\mathbf{A}_{i,\overline{id}_i^*}$, $i \in [l]$, використовуючи TrapGen з функцією з секретом $\mathbf{T}_{i,\overline{id}_i^*}$.

b. Будується вектор $\mathbf{u}$, з LWE задачі, $\mathbf{u} = \mathbf{w}_1$.

Відкриті параметри стають доступними зловмиснику.

2. Вироблення секретного ключа. Центр B відповідає на кожен запит вироблення секретного ключа для ідентифікатора id наступним чином:

a. Нехай $id \cap id^* := I \subset [l]$ і нехай $|I| = t < k$. Тоді, відмітимо, що B має функції з секретом для матриць відповідного набору $\overline{I}$, де $|\overline{I}| = l - t$. Припустимо, що перші t біти id дорівнюють id^*.

b. Символічно представимо частини $\mathbf{u}$, як $\hat{\mathbf{u}}_i = \mathbf{u} + \mathbf{a}_1 i + \mathbf{a}_2 i^2 + \ldots + \mathbf{a}_{k-1} i^{k-1}$, де кожен $\mathbf{a}_1,\ldots,\mathbf{a}_{k-1}$ є вектором змінної довжини n.

c. Для i, $id_i^* = id_i$, випадково обирається $\mathbf{e}_i$, використовуючи алгоритм SampleGaussian. Встановлюється $\mathbf{A}_{i,\mathrm{id}_i}\mathbf{e}_i$; $i \in [t]$.

d. Доки $t \le k-1$, і $k-1$ змінюється $\mathbf{a}_1,\ldots,\mathbf{a}_{k-1}$, випадково обирається $k-1-t$ частин з $\hat{\mathbf{u}}_{t+1},\ldots,\hat{\mathbf{u}}_{k-1}$, значення $\mathbf{a}_1,\ldots,\mathbf{a}_{k-1}$ є визначеними. Таким чином визначаються всі l частини $\hat{\mathbf{u}}_1,\ldots,\hat{\mathbf{u}}_l$.

e. Для знаходження $\mathbf{e}_j$, такі, що $\mathbf{A}_{j,\mathrm{id}_j}\mathbf{e}_j = \hat{\mathbf{u}}_j$, для $j = t+1,\ldots l$ застосовується алгоритм

$\mathbf{SamplePre}(\mathbf{A}_{j,\mathrm{id}_j}, \mathbf{T}_{j,\mathrm{id}_j}, \hat{\mathbf{u}}_j, \sigma)$.

f. Повертається $(\mathbf{e}_1,\ldots,\mathbf{e}_l)$.

Відмітимо, що розподіл відкритих параметрів і ключів в реальній схемі статистично не відрізняється від даної імітації.

3. Зашифрування повідомлення. A на виході має бітове повідомлення $b^* \in \{0, 1\}$. B на запит формує зашифрований текст для id^*:

a. Нехай $c_0 = Dv_1 + b\lfloor q/2 \rfloor$.

b. Нехай $c_i = (Dv_i^1, Dv_i^2, \ldots, Dv_i^m)$ для $i \in [l]$.

4. Розшифрування повідомлення. Зловмисник у якості вихідних даних має приблизне значення b'. Імітатор B використовує це припущення для визначення відповіді LWE оракула: якщо $b' = b^*$, тоді вихідне значення є «справжнім», інакше вихідне значення є «випадковим».

Вибір параметрів для нечітких IBE-схем на решітках

Для того, щоб результат дешифрування був коректним, та для забезпечення необхідного рівня захищеності, параметр безпеки n, верхня межа l, розмір множини та інші параметри, задаються при наступних обмеженнях [20]:

1. Для алгоритму генерування решітки з функцією з секретом необхідно, щоб $m \ge 5n\log q$. Враховуючи це обмеження для m, вихідною послідовністю алгоритму TrapGen є базис Грама-Шміта довжиною не більше $m \cdot \sqrt{\log m}$. Використовуючи алгоритм SamplePre, секретний ключ вектор $\mathbf{e}_j$, є взятим з дискретного рівняння Гауса зі стандартним відхиленням $\sigma \ge m \cdot \log m$, і, таким чином, з майже експоненціально малої ймовірністю, має довжину не більшу за $\sigma\sqrt{m} \le m^{1.5} \cdot \log m$.

2. Встановлюється розподілення з шумом $\chi = \bar{\Psi}_\alpha^m$, де $\alpha \ge 2\sqrt{m}/q$, до якого застосовується редукція Регева [19]. Вектор $\mathbf{x}$, вибраний з цього розподілення, має довжину $O(\alpha q\sqrt{m}) \le 2m$ з майже експоненціально малої ймовірністю.

3. Для коректності, необхідно, щоб задовольнялося рівняння:

$$|Dx - \sum_{j\in J} DL_j \mathbf{e}_j^{\mathrm{T}} \mathbf{x}_j| \le D|x| + \sum_{j\in J} D^2 |\mathbf{e}_j^{\mathrm{T}} \mathbf{x}_j| < q/4.$$

Оскільки $D = (l!)^2$, маємо:

$$|D|x| + \sum_{j\in J} D^2 |\mathbf{e}_j^{\mathrm{T}} \mathbf{x}_j| \le$$
$$\le D \cdot \alpha q\sqrt{m} + l \cdot D^2 \cdot (\alpha q\sqrt{m} \cdot m^{1.5} \log m \cdot \sqrt{m}) \le,$$
$$\le 4 \cdot m^3 \log m \cdot l(l!)^4 \le m^3 \log m \cdot 2^{5l}$$

причому, $(l!)^4 \le (l!)^{4l} \le 2^{5l}$. Параметр $q \ge m^3 \log m \cdot 2^{5l}$ забезпечує коректність.

Стосовно налаштування конкретних параметрів під ці обмеження, враховуючи постійну $\epsilon \in (0, 1)$, встановлюється:

- Параметр безпеки $n = l^{1/\epsilon}$.
- Модуль q повинен бути простим числом в інтервалі $[n^6 2^{5l}, 2 \cdot n^6 2^{5l}]$.
- $m = n^{1.5} \ge 5n\log q$, повинно задовольняти (1).

Проаналізувавши останні два пункти, можна побачити, що $q \ge m^3 \log m \cdot 2^{5l}$, а параметр шуму $\alpha = 2\sqrt{m}/q = 1/(2^{5n\epsilon} \cdot \mathrm{poly}(n))$.

Зв'язавши наведене вище, в найгіршому та середньому випадку, отримуємо захищеність, що відповідає стійкості $2^{O(n^\epsilon)}$-апроксимацій gapSVP або SIVP на n- мірних решітках, якщо використовувати алгоритми, що працюють в часі $q \cdot \mathrm{poly}(n) = 2^{O(n^\epsilon)}$. З даним рівнем знань алгоритм є LWE- стійким для $\epsilon < 1/2$.

6. ПОЄДНАННЯ МАТЕМАТИКИ АЛГЕБРАЇЧНИХ РЕШІТОК ЗІ СПАРЮВАННЯМИ ТОЧОК ЕК

Флоріан Гесс у роботі [21] запропонував математичний апарат, що поєднує математику спарювань точок ЕК та алгебраїчні решітки.

Для кільця A з ідеалом $I^{(i)}$ нехай, для зручності обчислень: $R=Z$ і $R=Q[t]$. Нехай R – домен (головний ідеал), і нехай $r,s\in R$, для $r\neq 0$, не рівних одиниці, і для s, що мають порядок $n\geq 2$ в $(R/rR)^{\times}$. Іншими словами, s – первісний корінь n-го ступеню з одиниці по модулю r.

Визначимо R-алгебру та її ідеали:

$$A=R[x]/(x^n-1)R[x],$$
$$I^{(i)}=\{h+(x^n-1)R[x]\,|\,h(s)\equiv 0 \bmod r^iR\}, \quad (1)$$

для $i\geq 0$, таких, що $s^n\equiv 1 \bmod r^iR$. Надалі елементи будуть ототожнюватися з їх поліноміальним представленням ступеню $\leq n-1$. Визначимо також R- модулі:

$$I^{(i),m}=\{h\in I^{(i)}\,|\,\deg(h)\leq m-1\}.$$

Відмітимо, що $I^{(i),m}\subseteq I^{(j),w}$, для $m\leq w$ і $j\leq i$, а також $I^{(i),n}=I^{(i)}$.

Структура ідеалу

Лема 1. *Ідеали $I^{(i)}$ та $I^{(i),m}$ мають наступні властивості:*

1. $I^{(i)}=r^iA+(x-s)A$.
2. $I^{(i),m}$ має вільний ранг m та базис $r^i, x-s, x^2-s^2,\ldots,x^{m-1}-s^{m-1}$.
3. Якщо $m\geq\phi(n)$, тоді $I^{(i),m}=M\oplus I^{(i),\phi(n)}$ з $M=\{h\in I^{(i),m}\,|\,h\equiv 0 \bmod \Phi_n\}$.

Доведення. З визначення $I^{(i)}$ ясно, що $r^iA+(x-s)A\subseteq I^{(i)}$. З іншого боку, нехай $h\in I^{(i)}$. Поліноміальний поділ $x-s$ із залишком показує, що $h=g\cdot(x-s)+h(s)$ з $g\in A$ і $h(s)\in R$. З визначення $I^{(i)}$ маємо $h(s)\in r^iR$. Отже, $h=h(s)+g\cdot(x-s)\in r^iA+(x-s)A$. Перше твердження доведене.

Друге твердження виводиться з першого та із короткої нормальної форми Ерміта, що обчислена над базисом $r^i, x-s, x(x-s),\ldots,x^{m-2}(x-s)$ для $I^{(i),m}$.

Трете твердження виводиться за допомогою поліноміального поділу Φ_n із залишком. Відображення $I^{(i),m}\to I^{(i),\phi(n)}$, $h\mapsto h \bmod \Phi_n$ ділиться на включення $I^{(i),\phi(n)}\to I^{(i),m}$. Де $\Phi_n\in I^{(i),\phi(n)}$, доки $\Phi_n(s)\equiv 0 \bmod r^i$. Відмітимо, що M – це вільний R-модуль з базисом $\Phi_n,\ldots,x^{m-\phi(n)-1}\Phi_n$.

Зазначимо, що додатково до Леми 1, можна показати, що $I^{(i)}=(I^{(1)})^i$, якщо $R=nR+rR$ (наприклад, якщо $R=Z$ і r – просте). Так як ідеал $I^{(i)}$ є замкнутим щодо множення на x, можна побачити, що він є замкнутим при обертанні коефіцієнтів $h\in I^{(i)}$.

Аргументи для решітки з $R=Z$

Нехай $R=Z$ та $r\geq 2$. Для $h=\sum_{i=0}^{d}h_ix^i\in Z[x]$, визначимо:

$$\|h\|_1=\sum_{i=0}^{d}|h_i| \quad\text{та}\quad \|h\|_2=\left(\sum_{i=0}^{d}|h_i|^2\right)^{1/2}.$$

Поширимо це визначення для A за допомогою представників класу ступенів $\leq n-1$. Це дозволить використовувати $I^{(i)}$ в математичних решітках. Маємо $\|\cdot\|_1=\Theta(\|\cdot\|_2)$ для $I^{(i)}$, де константи залежать тільки від n.

Лема 2. *Припустимо, що $i\geq 1$ задовольняє $s^n\equiv 1 \bmod r^i$ та нехай $h\in Z[x]$, так, що $h(s)\equiv 0 \bmod r^i$. Якщо $h\not\equiv 0 \bmod \Phi_n$, тоді:*

$$\|h\|_1\geq r^{i/\phi(n)}.$$

Доведення. Нехай ς – первісний корінь n- го ступеню з одиниці в $\bar{Q}$ і $B=Z[\varsigma]$ – кільце цілих чисел n-го ступеню поля циклотомічних чисел K/Q. Нехай $\alpha=r^iB+(\varsigma-s)B$. Тоді α – ідеал B з нормою $N_{K/Q}(\alpha)=r^i$, з припущенням по s. Маємо $\varsigma\equiv s \bmod \alpha$. Таким чином $h(\varsigma)\in\alpha\setminus\{0\}$ з припущенням по h, та, відповідно,

$$|N_{K/Q}(h(\varsigma))|\geq N_{K/Q}(\alpha)=r^i.$$

З іншого боку, $\phi(n)$ комплексно зв'язує $\varsigma^{(i)}$ з ς задовольняючи $|\varsigma^{(i)}|=1$. Тоді $|h(\varsigma^{(i)})|\leq\|h\|_1$ та:

$$|N_{K/Q}(h(\varsigma))|=|\prod_{j=1}^{\phi(n)}h(\varsigma^{(j)})|\leq\|h\|_1^{\phi(n)}$$

Об'єднання двох нерівностей доводить перше твердження.

Лема 3. *Припустимо, що $s^n\equiv 1 \bmod r^2$. Нехай $m\geq\phi(n)$ і $w=m-\phi(n)$. Будь-який LLL- зведений базис $v_1,\ldots,v_m$ над $I^{(1),m}$, з впорядкованої довжиною, задовольняє:*

$\|v_i\|_1=O(1)$ та $v_i\in I^{(2)}$, для $1\leq i\leq w$,

$\|v_i\|_1=\Theta(r^{1/\phi(n)})$ та $v_i\notin I^{(2)}$, для $w\leq i\leq m$.

Константи O і Θ залежать тільки від n і елемент, що співвідноситься з r, є достатньо великим порівняно з n.

Доведення. Згідно з Лемою 1, детермінантом $I^{(1),m}$ є r, з розмірністю m. Також, маємо $I^{(1),m}=M\oplus I^{(1),\phi(n)}$ з $M=\{h\in I^{(1),m}\,|\,h\equiv 0 \bmod \Phi_n\}$. Таким чином, існує хоча б $\phi(n)$ базисів векторів v_i над $I^{(1),m}$, що мають не нульові проекції на $I^{(1),\phi(n)}$. Згідно з Лемою 2, v_i задовольняють $\|v_i\|_2=\Omega(r^{1/\phi(n)})$. З іншого боку, LLL-властивість показує, що $\prod_{i=1}^{m}\|v_i\|_2=O(r)$. Таким чином, достеменно існує $\phi(n)$ базисів векторів v_i, з розміром $\Theta(r^{1/\phi(n)})$, що мають не нульові проекції на $I^{(1),\phi(n)}$. Інший базис векторів v_i в M та задовольняє $\|v_i\|_2=O(1)$. Оскільки v має задану довжину, звідси випливає і вибір норми.

Наразі $\Phi_n(s)\equiv 0 \bmod r^2$ за припущенням по s. Отже $v\in I^{(2)}$ для будь якого $v\in M$. Тоді, $v_i\in I^{(2)}$ для $1\leq i\leq w$. З іншого боку, якщо $v\in I^{(1),m}\setminus M$ та $v\in I^{(2)}$, тоді $v\not\equiv 0 \bmod {}_n^{\mathrm{l}}$ та $v(s)\equiv 0 \bmod r^2$. Тоді, згідно з Лемою 2, $\|v\|_2=\Omega(r^{2/\phi(n)})$, чого не може бути. Звідси, $v_i\notin I^{(2)}$ для $w\leq i\leq m$.

Дійсні константи O-термів і Θ-термів є важко обчислюваними, та є доступними тільки за умови обмежень гіршого випадку, які, зазвичай, занадто великі. Оскільки на практиці r є значно більшим за n, вплив цього терму є настільки малим, що ним можна знехтувати. У цьому випадку залежності елемента зберігаються. Відмітимо, що будь-який LLL-зведений базис $I^{(1),m}$ повинен містити хоча б один базисний елемент, що не належить до $I^{(2)}$.

Аргументи для решітки з $R=Q[t]$

Нехай $R=Q[t]$ і $\deg(r)\ge 1$.

Для $h=\sum_{i=0}^{d} h_i x^i \in Q[t,x]$, з $h_i = Q[t]$ визначимо:

$$\deg_t h = \max_{0\le i\le d} \deg(h_i).$$

Поширимо це визначення для A за допомогою представників класу x ступенів $\le n-1$. Це дозволить використовувати $I^{(i)}$ в математичних решітках зі ступенем (мається на увазі, що $I^{(i)}$ – вільний $Q[t]$-модуль кінцевого рангу, підмножини якого обмежені значеннями ступенів кінцевовимірного простору векторів).

Лема 4. *Припустимо, що $i\ge 1$ задовольняє $s^n \equiv 1 \bmod r^i Q[t]$ та нехай $h\in Q[t,x]$, так, що $h(s)\equiv 0 \bmod r^i Q[t]$. Якщо $h\not\equiv 0 \bmod \Phi_n(x) Q[t,x]$, тоді:*

$$\deg_t(h) \ge i/\phi(n)\deg(r).$$

Доведення. Нехай ς – первісний корінь n-го ступеню з одиниці в $\bar{Q}$ і $B=Q[t,\varsigma]$ – ціле замикання $Q[t]$ в функціональному полі $K=Q(t,\varsigma)/Q$. Нехай $\alpha = r^i B + (\varsigma - s)B$. Тоді α – ідеал B з нормою $N_{K/Q}(\alpha)=r^i$, з припущенням по s. Маємо $\varsigma \equiv s \bmod \alpha$. Таким чином $h(\varsigma)\in\alpha$ з припущенням по h, та, відповідно:

$$\begin{aligned}\deg(N_{K/Q(t)}(h(\varsigma))) &\ge \deg(N_{K/Q(t)}(\alpha)) = \\ &= i\deg(r)\end{aligned} \quad (1)$$

З іншого боку, $\phi(n)$ розкладання Пюїзе в ряд ς за ступенем оцінки $Q(t)$ є майже сталою (часто без ненульових ступенів t), комплексно пов'язаних $\varsigma^{(i)}$ з ς, і тим самим задовольняє $\deg(\varsigma^{(i)})=0$. Тоді $\deg(h(\varsigma^{(i)})) \le \deg_t(h)$ та:

$$\deg(N_{K/Q}(h(\varsigma))) = \deg\left(\prod_{j=1}^{\phi(n)} h(\varsigma^{(j)})\right) =$$

$$= \prod_{j=1}^{\phi(n)} \deg(h(\varsigma^{(j)})) \le \phi(n)\deg_t(h).$$

Об'єднання двох нерівностей доводить дане твердження.

Наступна Лема використовує функціональні поля LLL. Вхідними значення $M\in Q[t]^{n\times n}$ з $\det(M)\ne 0$ функціонального поля LLL виходів $N,T\in Q[t]^{n\times n}$, такі, що $N=MT, \det(T)=1$ та сума максимальних ступенів в кожному стовпці $\det(M)$. Стовпці N є за визначенням LLL-зведеними елементами $Q[t]^n$.

Лема 5. *Припустимо, що $s^n \equiv 1 \bmod r^2 Q[t]$. Нехай $m\ge\phi(n)$ та $w=m-\phi(n)$. Будь-який упорядкований по довжині LLL-зведений базис $v_1,\dots,v_m$ над $I^{(1),m}$, задовольняє:*

$\deg_t v_i = 0$ та $v_i \in I^{(2)}$, для $1\le i\le w$,

$\deg_t(v_i) = 1/\phi(n)\deg(r)$ та $v_i \notin I^{(2)}$, для $w\le i\le m$.

Доведення. Доведення даної леми є в точності аналогічним доведенню Леми 3 (за аналогію використовується $\deg_t = (\|\cdot\|_2)$).

Спарювання на решітках

Нехай V_n – мультиплікативна група, вигляду:

$$V_n = \{wf \mid w\in F_q \cap \mu_{lcm(2,n)}, \\ f: G_1\times G_2 \to \mu_r\}$$

де G_1 та G_2 – циклічні групи простого порядку r та $\gcd(n,r)=1$. Нехай W_n позначає фактор групи V_n, обчислений шляхом факторизації константних функцій зі значеннями в $F_q\cap\mu_{\mathrm{lcm}(2,n)}$. Тоді елементами W_n є функції $G_1\times G_2\to\mu_r$, які визначені з точністю до скалярних кратних з $F_q\cap\mu_{\mathrm{lcm}(2,n)}$. Нехай W_n^{bilin} позначає підгрупу W_n, що генерована шляхом використання білінійних функцій.

Теорема 1. *Нехай r – просте число, взаємно просте з n, та s – примітивний корінь n-го ступеню з одиниці по модулю r^2. Нехай:*

$$a_s: I^{(1)} \to W_n, \quad h \mapsto a_{s,h}$$

буде відображенням, з наступними властивостями:

1. $a_{s,g+h} = a_{s,g}a_{s,h}$ *для всіх* $g,h\in I^{(1)}$;
2. $a_{s,hx} = a_{s,h}^s$ *для всіх* $h\in I^{(1)}$ *з* $a_{s,h}\in W_n^{bilin}$;
3. $a_{s,r}\in W_n^{bilin}\setminus\{1\}$ *та* $a_{s,t-s}=1$.

Тоді $\mathrm{im}(a_s)\in W_n^{bilin}$ *та* $\ker(a_s)=I^{(2)}$. *Точніше,* $a_{s,h}=a_{s,r}^{h(s)/r}$, *для всіх* $h\in I^{(1)}$.

Існує ефективно обчислюване $h\in I^{(1),\phi(n)}$ *з* $\|h\|_1 \ge O(r^{1/\phi(n)})$ *та* $a_{s,h}\ne 1$. *Константа O залежить тільки від n.*

Будь-яке $h\in I^{(1)}$ *з* $a_{s,h}\ne 1$ *задовольняє* $\|h\|_1 \ge r^{1/\phi(n)}$.

Доведення. З першої та другої властивостей можна побачити, що $a_{s,hg}=a_{s,h}^{g(s)}$ для всіх $h\in I^{(1)}$ з $a_{s,h}\in W_n^{bilin}$ і $g\in A$. З Леми 1, маємо $I^{(1)} = rA + (x-s)A$, отже, кожне $h\in I^{(1)}$ має вигляд $h=g_1 r + g_2(x-s)$ з $g_1,g_2\in A$. Тоді, використовуючи третю властивість можна обчислити:

$$a_{s,h} = a_{s,g_1 r + g_2(x-s)} = \\ = a_{s,r}^{g_1(s)} a_{s,x-s}^{g_2(s)} = a_{s,r}^{g_1(s)} \in W_n^{bilin}$$

і, отже, $\mathrm{im}(a_s)\subseteq W_n^{bilin}$. Доки $a_{s,r}\ne 1$ та r – просте, маємо $\mathrm{im}(a_s)\in W_n^{bilin}$.

Властивості a_s показують до яких пір можна спростити вираз. Беремо W_n^{bilin} за A-модулем,

через $f^g = f^{g(s)}$ для $f \in W_n^{bilin}$ та $g \in A$. Тоді a_s – епіморфізм з A-модулями $I^{(1)}$ і W_n^{bilin}.

Ядром a_s є A-подмодуль $I^{(1)}$ і, отже, ідеал A міститься в $I^{(1)}$. Оскільки a_s сюр'єктивно, індекс задовольняє $(I^{(1)} : \ker(a_s)) = \#W_n^{bilin} = r$. Але $r^2, x - s \in \ker(a_s)$, тоді за Лемою 1 $I^{(2)} = r^2 A + (x - s)A \subseteq \ker(a_s)$. Також з Леми 1 маємо $(I^{(1)} : I^{(2)}) = r$, отже $\ker(a_s) = I^{(2)}$.

З формули (1.1) можна побачити, що $g_1(s) = h(s)/r \bmod r$, і, отже $a_{s,h} = a_{s,r}^{h(s)/r}$, що показує зв'язок $a_{s,h}$ з генератором $a_{s,r} \in W_n^{bilin}$.

Використовуючи $\ker(a_s) = I^{(2)}$, інша частина теореми безпосередньо випливає з Леми 3 (враховуючи $m = \varphi(n)$), LLL-алгоритму і Леми 2.

Ідеал $I^{(1)}$ разом з відображенням $a_s : I^{(1)} \to W_n$, що задовольняє властивостям наведеним в Теоремі 1, називають спарюванням на решітці зі функцією спарювання решітки a_s.

Теорема 2. *Нехай $n \geq 2$ та r, s – змінні поліноми в $Z[t]$, такі, що s – примітивний корінь n-го ступеню з одиниці по модулю r^2, а r – примітивний поліном. припустимо також, що існує функція спарювання решітки:*

$$a_{s(t_0)} : I^{(1)}_{r(t_0),s(t_0)} \to W^{bilin}_{n,r(t_0)},$$

для всіх $t_0 \in J$, де J – відповідна необмежена підмножина Z.

Тоді існує $h \in Z[t][x]$ з $\deg(h) \leq \phi(n) - 1$ та $\deg_t(h) = 1/\phi(n)\deg(r)$, таке, що: $a_{s(t_0),h(t_0,x)} \neq 1$, для всіх досить великих $t_0 \in J$. Поліном h можна ефективно обчислити.

Будь-який $h \in Z[t][x]$, такий, що $a_{s(t_0),h(t_0,x)} \neq 1$, для всіх досить великих $t_0 \in J$, задовольняє умові $\deg_t(h) \geq 1/\phi(n)\deg(r)$.

Доведення. Існує лише кінцеве число $t_0 \in J$, таких, що $s(t_0)$, що мають порядок менший за $n \bmod r^2$, так як t_0 повинні бути нулями за $s^m - 1 \bmod r$ для $m < n$. Доки t_0 обирається досить великим, можна вважати, що $s(t_0)$ – примітивний корінь n-го ступеню з одиниці по модулю r^2.

Відповідно до початку цього розділу, визначимо $A, I^{(1)}, I^{(2)}$ для r, s і $R = Q[t]$. З властивості Леми 5 $m = \varphi(n)$ і функції LLL- поля, можна побачити, що існують $v_i \in Q[t][x]$ з $v_i(s) \equiv 0 \bmod rQ[t]$, $\deg(v_i) \leq \varphi(n) - 1$ та $\deg_t(v_i) = 1/\phi(n)\deg(r)$ для $1 \leq i \leq \phi(n)$. Нехай $h \in Z[t][x]$ буде добутком v_i з найменшим спільним кратним всіх знаменників усіх Q-коефіцієнтів v_i. Тоді з Леми Гауса, $h(s) \in Z[t]$ та $h(s) \equiv 0 \bmod rZ[t]$, оскільки r вважається примітивним.

Підставляючи в порівняння t_0 замість t, маємо $h(t_0, s(t_0)) \equiv 0 \bmod r(t_0)$. З $\deg_t(h) = 1/\phi(n)\deg(r)$ можна побачити $\|h(t_0, x)\|_1 = O(r(t_0)^{1/\phi(n)})$. З Леми 2 випливає, що $h(t_0, s(t_0)) \not\equiv 0 \bmod r(t_0)^2$. Робимо висновок, що $a_{s(t_0),h(t_0,x)}$ визначає не вироджене спарювання.

Останнє твердження про ступінь випливає з $\|h(t_0, x)\|_1 \geq r(t_0)^{1/\phi(n)}$ за Лемою 2, якщо t_0 прагне до нескінченності.

ВИСНОВКИ ТА ПРОПОЗИЦІЇ

Більшість існуючих схем, що базуються на ідентифікаторах, використовують математику білінійних відображень точок на еліптичних кривих. Складність даних перетворень базується на вирішенні задачі дискретного логарифму в групі точок еліптичної кривої, та знаходься в межах між субекспоненційною і експоненційною. Криптографічні алгоритми, що базуються на спарюваннях, не мають прийнятної швидкодії.

Альтернативою математиці спарюванням точок є математика, що використовує перетворення в кільцях зрізаних поліномів – алгебраїчні решітки. Дані обчислення мають лінійну складність обчислень, яка дорівнює $O(n2)$, що забезпечує швидкодію обчислень. Криптографічна стійкість таких алгоритмів ґрунтується на складності вирішенні задачі знаходження найкоротшого вектора в заданій решітці. На даний момент не існує алгоритмів, які б знаходили найкоротший вектор зі складністю меншу за експоненційну.

Таким чином, до основних переваг криптосистем на решітках можна віднести швидкодію, що є наближеною до швидкодії симетричних алгоритмів, за умови використання розпаралелювання, а також стійкість до атак з використанням навіть квантових обчислень. Але дані системи мають і недоліки, основним з яких є занадто великий розмір ключів та зашифрованого тексту.

Проаналізувавши основні IBE-схеми, що використовують алгебраїчні решітки, можна відмітити, що:

1. Схеми на основі функцій з секретом, з обраним прообразом, тобто з підібраним базисом за допомогою розподілення Гауса, зі стандартним відхиленням, що наближається до найбільшого з векторів Грама-Шмита, отриманих завдяки ортогоналізації цього базису, забезпечують складність найгіршого випадку вирішення задачі на решітках, в моделі випадкового оракулу.

2. Складність схем, що базуються на вирішенні LWE-задачі, заснована найгіршому випадку квантової складності наближеної SVP-задачі. Що означає, що розкриття таких схем тягне за собою появу ефективних квантових алгоритмів вирішення наближеної SVP-задачі, що є малоймовірним. Квантова обчислювальна модель використовується тільки при зведенні задач теорії решіток до LWE-задач, сама LWE-задача, так само, як і всі системи шифрування засновані на ній, використовує класичну обчислювальну модель.

3. Системи шифрування засновані на LWE-задачах мають деяку невелику ймовірність помилки дешифрування повідомлення, що зменшується, завдяки правильно підібраним параметрам (див. пункт 5). Також, цю ймовірність можна зменшити

до несуттєвої, завдяки використанню завадостійкого кодування до етапу зашифрування.

4. Алгоритми шифрування засновані на LWE- задачах мають наступні властивості:

- розміри секретного ключа $nl\log q$;
- розмір відкритого ключа $m(n+l)\log q$;
- розмір повідомлення $l\log t$;
- розмір зашифрованого тексту $(n+l)\log q$;
- зашифрування веде до росту повідомлення у $(1+\frac{n}{l})\log q / \log t$ разів;
- для зашифрування одного біту повідомлення необхідно $\tilde{O}(m(1+\frac{n}{l}))$ операцій;
- для розшифрування одного біту повідомлення необхідно $\tilde{O}(n)$ операцій.

В подальшому повинні бути вирішеними такі проблемні питання і задачі.

1. Теоретичні дослідження існуючих криптографічних алгоритмів на ідентифікаторах, що використовують математичні решітки.

2. Обґрунтування та побудування захищеної криптографічної схеми на основі математики алгебраїчних решіток.

3. Удосконалення IBE-систем шифрування на решітках, зокрема методів оптимізації довжини ключового матеріалу, за допомогою використання структурних циклічних решіток.

4. Зіставлення алгоритмів шифрування на решітках з алгоритмами шифрування на основі теоретики-числових проблем. Так, якщо існує оракул, що вирішує $\sqrt{n}$ -наближені SVP-задачі факторизації цілого числа, або дискретного логарифму, тоді алгоритми на решітках є більш крипто стійкими, ніж алгоритми на основі теоретики-числових проблем.

5. Пошук методів та засобів оцінки, обґрунтування критеріїв IBE-алгоритмів, що використовують алгебраїчні решітки.

6. Подальші дослідження стосовно можливості побудування алгоритмів на основі поєднання математик алгебраїчних решіток і спарювань точок еліптичних кривих.

Література

[1] *Clifford Cocks.* An identity based encryption scheme based on quadratic residues / In Bahram Honary edit. // IMA Int. Conf. «Lecture Notes in Computer Science». – Vol.2260. – Springer. – 2001. – P.360–363.

[2] *Dan Boneh.* Space-efficient identity based encryption without pairings / Dan Boneh, Craig Gentry, Michael Hamburg // IEEE Computer Society, FOCS. – 2007. – P.647–657.

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

[4] *Shweta Agrawal.* Efficient lattice (H)IBE in the standard model / Shweta Agrawal, Dan Boneh, Xavier Boyen // In Henri Gilbert edit. – EUROCRYPT Int. Conf. «Lecture Notes in Computer Science». – Vol.6110. – Springer. – 2010. – P.553-572.

[5] *Dan Boneh, Matthew K. Franklin.* Identity-based encryp tion from the Weil pairing / Dan Boneh, Matthew K. Franklin // SIAM Journal on Computing. – Vol. 32(3). – 2003. – P.586-615.

[6] *Chris Peikert.* Bonsai trees (or, arboriculture in lattice-based cryptography) [Електронний ресурс] / Chris Peikert // Cryptology ePrint Archive. – Report 2009/359. – 2009. – Режим доступу: http://eprint.iacr.org/.

[7] *Shweta Agrawal.* Lattice basis delegation in fixed dimension and shorter -ciphertext hierarchical IBE / Shweta Agrawal, Dan Boneh, Xavier Boyen // In Tal Rabin edit. – CRYPTO «Lecture Notes in Computer Science». – Vol.6223. – Springer. – 2010. – P.98-115.

[8] *Miklos Ajtai.* Generating hard instances of the short basis problem / Miklos Ajtai // In Jirэ Wiedermann, Peter van Emde Boas, Mogens Nielsen edit. – ICALP «Lecture Notes in Computer Science». – Vol.1644. – Springer. – 1999. – P.1-9.

[9] *Amit Sahai, Brent Waters.* Fuzzy identity-based encryption / Amit Sahai, Brent Waters // EUROCRYPT. – 2005. – P.457-473.

[10] *Jonathan Katz.* Predicate encryption supporting disjunctions, polynomial equations, and inner products / Jonathan Katz, Amit Sahai, Brent Waters // EUROCRYPT'08 «Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology» – Springer-VerlagBerlin, Heidelberg – 2008. – P.146-162.

[11] *Allison B. Lewko.* Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption / Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, Brent Waters // EUROCRYPT. – 2010. – P.62-91.

[12] *John Bethencourt.* Ciphertext-policy attribute-based encryption / John Bethencourt, Amit Sahai, Brent Waters // In SP '07 «Proceedings of the 2007 IEEE Symposium on Security and Privacy». – IEEE Computer Society. – Washington, DC, USA. – 2007. – P.321-334.

[13] *Ling Cheung, Calvin C. Newport.* Provably secure ciphertext policy ABE / Ling Cheung, Calvin C. Newport // ACM conference Computer and Communications Security. – 2007. – P.456-465.

[14] *Vipul Goyal.* Attribute-based encryption for fine-grained access control of encrypted data / Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters // CCS '06 «Proceedings of the 13th ACM conference on Computer and communications security». – ACM. –New York, USA – 2006. – P.89–98.

[15] *Allison B. Lewko.* Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption / Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, Brent Waters // EUROCRYPT. – 2010. – P.62-91.

[16] *Allison B. Lewko, Brent Waters.* Unbounded HIBE and attribute-based encryption / Allison B. Lewko, Brent Waters // EUROCRYPT. – 2011. – P.547-567.

[17] *Rafail Ostrovsky.* Attribute-based encryption with non-monotonic access structures / Rafail Ostrovsky, Amit Sahai, Brent Waters // CCS '07 «Proceedings of the 14th ACM conference on Computer and communications security». – ACM. –New York, USA – 2007. – P.195–203.

[18] *Shweta Agrawal*. Fuzzy Identity Based Encryption from Lattices [Електронний ресурс] / Shweta Agrawal, Xavier Boyen, Vinod Vaikuntanathan, Panagiotis Voulgaris, Hoeteck Wee // Cryptology ePrint Archive. – Report 2011/414. – 2011. – Режим доступу: http://eprint.iacr.org/.

[19] *Daniele Micciancio, Oded Regev*. Worst-case to average-case reductions based on Gaussian measures / Daniele Micciancio, Oded Regev // FOCS '04 «Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science». – IEEE Computer Society. – Washington, DC, USA. – 2004. – P.372-381.

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

[21] *Florian Hess*. Pairing Lattices [Електронний ресурс] / Florian Hess // Cryptology ePrint Archive: Report 2008/125. – 2008. – Режим доступу: http://eprint.iacr.org/.

[22] *Daniele Micciancio, Oded Regev*. Lattice-based Cryptography // Daniele Micciancio, Oded Regev /In D.J. Bernstein; J. Buchmann; E. Dahmen edit. – «Post Quantum Cryptography». – Springer. – 2009. – P.147-191.

Надійшла до редколегії 2.03.2012

Горбенко Іван Дмитрович, фото та відомості про автора див. на с. 190.

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

УДК 004.056.55

Анализ криптографических алгоритмов на идентификаторах, использующих алгебраические решетки / И.Д. Горбенко, Л.В. Макутонина, // Прикладная радиоэлектроника: науч.-техн. журнал. – 2012. – Том 11. № 2. – С. 200–209.

Приводятся результаты анализа существующих алгоритмов на идентификаторах, использующих алгебраические решетки. Обосновываются выбор параметров, для обеспечения необходимого уровня защищенности. Излагается доказательство безопасности относительно задачи обучения с ошибками в модели случайного оракула.

Ключевые слова: криптографические системы на идентификаторах, алгебраические решетки, алгоритм зашифрования, алгоритм розшифрования, идентификатор пользователя, прообраз выборки, функция с секретом.

Библиогр.: 22 назв.

UDK 004.056.55

Analysis of identity-based cryptographic algorithms using algebraic lattices / I.D. Gorbenko, L.V. Makutonina, // Applied Radio Electronics: Sci. Journ. – 2012. Vol. 11. № 2. – P. 200–209.

The results of the analysis of existing identity-based cryptographic algorithms using algebraic lattices are given. The choice of parameters to ensure the necessary level of security is grounded. The proof of safety with respect to the problem of learning with errors in a random oracle model is presented.

Keywords: identity-based encryption systems, algebraic lattices, encryption algorithm, decryption algorithm, user ID, sampling preimage, trapdoor function.

Ref.: 22 items.