Лабораторная работа № 4

Криптоанализ схемы шифрования Kyber

Дедлайн: 20.05.2024

1 LWE и решетки

Рассмотрим классическую задачу LWE: по заданным $(A, \mathbf{b} = A\mathbf{s} + \mathbf{s}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$, найти $\mathbf{s} \in \mathbb{Z}_q^n$ (или $\mathbf{e} \in \mathbb{Z}_q^m$), где оба вектора $\mathbf{s}, \mathbf{e}$ ограничены по евклидовой длине. Задача напрямую связана с задачей BDD на решетках конструкции-A, то есть на решетках вида

$$\mathcal{L}(A) = \{\mathbf{x} \in \mathbb{Z}^m, \exists \mathbf{c} \in \mathbb{Z}^n \ : \ \mathbf{x} = A\mathbf{c} \bmod q\}.$$

Вторая компонента выборки LWE – вектор $\mathbf{b}$ – отстает от вектора $A\mathbf{s}$ решетки $\mathcal{L}(A)$ на $\|\mathbf{e}\|$. Заметим, что $\|\mathbf{e}\| \leq \lambda_1(\mathcal{L}(A)) \approx \sqrt{m}q^{1-n/m}$ (подумайте, откуда взялась последняя аппроксимация), отсюда получаем BDD инстанцию.

2 Эффективная версия криптосистемы Регёва

Основная операция в классической криптосистеме Регёва и некоторых её модификаций – это умножение матрицы на вектор. Например, для получения публичного ключа, публичная матрица $A \in \mathbb{Z}_q^{m\times n}$ умножается на секретный вектор $\mathbf{s}$ и к результату добавляется шум. В генерации шифр-текста также используется произведение матрицы A на короткие вектора. Таким образом, в криптосистемах на классическом LWE ключ занимает порядка $\mathcal{O}(n \cdot m \log q)$ бит, а умножение матрицы на вектор занимает квадратичное от n время. На практике для безопасных параметров такой размер ключа и такие временные затраты неэффективны. Поэтому в 2015 году Stehlé-Langlois [1] предложили задачу Module-LWE. Идея – заменить кольцо $\mathbb{Z}_q$ на кольцо многочленов $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$. Обычно n выбирается степенью двойки, и тогда такое кольцо является фактор-кольцом кольца целых циклотомического поля $\mathbb{Q}(x)/(x^n + 1)$.

Под $\mathbf{x} \in \mathcal{R}_q^k$ для целого $k \geq 1$ будем понимать вектор $\mathbf{x}$, координаты которого – многочлены из $\mathcal{R}_q$. Задача Module-LWE формулируется следующим образом:

Определение 1 (Module-LWE)**.** *По заданным двойкам* $(\mathbf{a}_1, \langle \mathbf{a}_1, \mathbf{s}\rangle + \mathbf{e}_1), \ldots, (\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s}\rangle + \mathbf{e}_m)$*, где*

- m *произвольное целое*
- $\mathbf{s} \in \mathcal{R}_q^k$ *взято либо случайно равномерно, либо из Гауссового распределения (по-коэффициентно)*
- $\mathbf{a}_i \in \mathcal{R}_q^k$ *взяты из случайного равномерного распределения (по-коэффициентно из* $\mathbb{Z}_q$*)*
- *коэффициенты* $\mathbf{e}_i$ *взяты из Гауссового распределения,*

следует найти $\mathbf{s}$*.*

Задачу Module-LWE теперь можно рассматриваться как задачу BDD над модулем

$$M = \{\mathbf{x} \in \mathcal{R}^m, \exists \mathbf{c} \in \mathcal{R}^k \ : \ \mathbf{x} = A\mathbf{c} \bmod q\}, \quad \text{где } \mathcal{R} = \mathbb{Z}[x]/(x^n + 1).$$

На практике такие модули дают, во-первых, уменьшение размера ключа, а во-вторых, ускорение в генерации ключей и шифр-текстов: умножение многочленов эффективнее (при помощи преобразования Фурье и подобных трюков) умножения векторов.

Заметим, что многочленам из $\mathcal{R}_q$ можно уникальным образом сопоставить вектора из $\mathbb{Z}_q^n$:

$$a_0 + a_1 x + \dots a_{n-1} x^{n-1} \mapsto (a_0, a_1, \dots, a_{n-1}),$$

а значит, и Module-LWE можно рассматривать как задачу нахождения ближайшего вектора над $\mathbb{Z}^{k \cdot n}$. Имея в виду такое отображение, мы будем обозначать вектора, состоящие только из одного многочлена, жирным шрифтом, понимая, что они могут быть рассмотрены как вектора над $\mathbb{Z}$.

Для примера рассмотрим $k = 1$ (такая версия Module-LWE называется Ring-LWE и исторически была предложена до Module-LWE [2, 3]). Имеем выборку $(\mathbf{a}, \mathbf{b} = \mathbf{as} + \mathbf{e} \bmod q)$. Для фиксированного многочлена $\mathbf{a} \in \mathbb{Z}[x]/(x^n + 1)$, умножение на этот многочлен можно описать умножением матрицы $\mathsf{Rot}(a)$ на вектор-коэффициентов второго множителя, где

$$\mathsf{Rot}(\mathbf{a}) = [x^{j-1} a \bmod (x^n + 1)]_{0 \le j \le n-1} = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ -a_{n-1} & a_0 & \dots & a_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & \dots & a_0 \end{pmatrix},$$

а результат умножения $\mathbf{ay}$ для произвольного $\mathbf{y} \in \mathbb{Z}[x]/(x^n + 1)$ есть многочлен, составленный из коэффициентов $\mathsf{Rot}(\mathbf{a})(y_0, \dots, y_{n-1})$ (можете проверить на примере). Матрицы $\mathsf{Rot}(a)$, составленные таким образом, называются анти-циркулянтными. Таким образом, Module-LWE выборка $(\mathbf{a}, \mathbf{b})$ может быть описана как пара

$$(\mathsf{Rot}(\mathbf{a}), \mathsf{Rot}(\mathbf{a}) \cdot (s_0, \dots, s_{n-1}) + (e_0, \dots, e_{n-1})) \in \mathbb{Z}_q^{n \times n} \times \mathbb{Z}_q^n.$$

Заметим, что лишь одна пара многочленов $(\mathbf{a}, \mathbf{b})$ генерирует n сэмплов классического LWE.

Для $k > 1$, module-LWE описывается матрицей из $\mathbb{Z}_q^{nk}$, на главной диагонали которой стоят блоки $\mathsf{Rot}(a_i)$, например:

$$\left(\begin{array}{c|c} \mathsf{Rot}(\mathbf{a}_1) & \mathbf{0} \\ \hline \mathbf{0} & \mathsf{Rot}(\mathbf{a}_2) \end{array}\right) \in \mathbb{Z}_q^{2n \times 2n}.$$

3 Kyber

Криптосистема Kyber [4] – это версия криптосистемы Регёва, перенесенная на Module-LWE. В качестве публичного ключа генерируются $A \in \mathcal{R}_q^{k \times k}, \mathbf{t} = A\mathbf{s} + \mathbf{e} \in \mathcal{R}_q^k$. Шифр-текст вычисляется аналогично классической криптосистеме, где вместо малых векторов над $\mathbb{Z}_q^n$ или $\mathbb{Z}_q^m$, генерируются вектора многочленов с малыми коэффициентами. В итоге, шифр-текст есть пара $(\mathbf{c}_1, \mathbf{c}_2) \in \mathcal{R}_q^k \times \mathcal{R}_q$.

4 Задание

Публичные чалленджи, посвященные криптосистеме Kyber, предложены Рурским Университетом г. Бохум и доступны по адресу `https://bochum-challeng.es/challenges/kyber`. Чалленджи отсортированы по сложности (см. "bit complexity"). Задача лабораторной состоит в решении простых чалленждей (для них достаточно запуска BKZ редукции с алгоритмом Enumeration, как реализовано в fpylll), а именно задач битовой сложности 16.[1] Для решения одного чалленджа необходимо:

[1] Группа, решившая чаллендж с битовой сложностью 32 и выше (Kyber-192-k12 и выше), получает Отлично автоматом по курсу.

1. скачать файл формата .py одного из параметров. В нём вы увидите среди прочих параметры n, k, q, публичную матрицу $A \in \mathcal{R}_q^{k \times k}$ (записанную как трехмерный массив – матрица, состоящая из многочленов), открытая компонента ключа $\mathbf{t} \in \mathcal{R}_q^k$, и множество шифр-текстов: каждый шифр-текст – это массив, состоящий из двух элементов: $\mathbf{c}_1 \in \mathcal{R}_q^k$ (поэтому $\mathbf{c}_1$ – это двумерных массив из k векторов длины n), и $\mathbf{c}_2 \in \mathcal{R}_q$ (одномерный массив из n элементов).

2. Получить из $A, \mathbf{t}$ секретный ключ $\mathbf{s}$, решая задачу BDD. Вы можете использовать метод редукции BDD к uSVP, описанный в лекции 8 `https://crypto-kantiana.com/elena.kirshanova/teaching/lattices_2024/Lecture8.pdf`. [2]

3. Получив секретный ключ, вам необходимо дешифровать все шифр-тексты для данного челленджа. Если вы преобразуете полученные сообщения в текст (кодировка UTF-8), у вас должен получится связных английский текст.

Список литературы

[1] Adeline Langlois and Damien Stehlé. *Worst-Case to Average-Case Reductions for Module Lattices* `https://eprint.iacr.org/2012/090`

[2] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. *On Ideal Lattices and Learning with Errors Over Rings* `https://eprint.iacr.org/2012/230.pdf`

[3] Damien Stehlé and Ron Steinfeld. *Making NTRUEncrypt and NTRUSign as Secure as Standard Worst-Case Problems over Ideal Lattices* `https://eprint.iacr.org/2013/004`

[4] Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancréde Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehé. *CRYSTALS - Kyber: A CCA-secure module-lattice-based KEM* `https://eprint.iacr.org/2017/634.pdf`

[2] при составлении базиса решетки не забудьте q-арные вектора!