Е. Киршанова БФУ им. И.Канта

Контрольная работа

по дисциплине

Криптография на решетках

2021–2022

Время: 200 минут + 10 минут на скан и отправку
31.05.2021

Имя : _____

Фамилия : _____

Требования:

- Решения можно записывать, либо используя этот темплейт, либо отдельные листы с четким указанием, к какому заданию относится решение. Первую страницу заполнять необязательно.
- Пишите **разборчиво**.
- Присылать решения (желательно в файлах формата .pdf или .jpeg **адекватного** размера) на почту elenakirshanova@gmail.com
  Решение задания №4 присылать в формате **.sage**
- Время начала экзамена: **8:30**, ответы на почту принимаются строго до **12:00**.

Задание	1	2	3	4
Баллы	/ 6	/ 5	/ 5	/ 5

Задание 1. Тривиальные задачки (3×2 баллов)

1 Пусть решетка $L \subset \mathbb{Z}^3$ задана как

$$L = \{v \in \mathbb{Z}^3 \ : \ v_1 + v_2 + v_3 = 0 \bmod 3\}.$$

Найдите кратчайший ненулевой вектор решетки L в евклидовой норме (ℓ_2)

2 Рассмотрим решетку, порожденную столбцами матрицы

$$B = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Опишите все последовательные минимумы этой решетки в норме ℓ_∞ (напомним, $\|x\|_\infty = \max_i |x_i|$), а также вектора, достигающие эти минимумы.

3 Опишите эффективный алгоритм, который по заданному базису B решётки определяет, является ли решетка $L(B)$ циклической. Решетка $L(B)$ называется циклической, если все ротации вектора $\vec{x}$ лежат в $L(B)$, т.е. $(x_1, \ldots, x_n) \in L(B) \iff (x_n, x_1, \ldots, x_{n-1}) \in L(B)$. Пример циклической решетки: $L(B)$, где $B = \begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

Задание 2. Определитель дуальной решетки (5 баллов)
Покажите, что $\det(\hat{L}) = \frac{1}{\det(L)}$, где $\hat{L}$ – решетка, дуальная к L.

Задание 3. Легкая версия LWE (5 баллов)

Пусть $q = 2^\ell$. Рассмотрим вариацию задачи LWE, в которой, вместо $\vec{a} \xleftarrow{\$} \mathbb{Z}_q^n$, мы будем умножать фиксированное секретное значение (скаляр) $s \in \mathbb{Z}_q$ на вектор-гаджет $\vec{g} = [1, 2, 4, \ldots, 2^{\ell-1}]$. Иными словами, нам дано

$$(\vec{g}, \vec{b} = s \cdot \vec{g} + \vec{e} \bmod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^n,$$

где $e \in \left[-\frac{q}{4}, \frac{q}{4}\right)^n$ – вектор-ошибка. Покажите, как по данным значениям $(\vec{g}, \vec{b})$, можно эффективно найти s. Обобщите результат для гаджета-матрицы $G = \mathsf{Id}_n \otimes \vec{g} = \mathsf{diag}(\vec{g}, \ldots, \vec{g}) \in \mathbb{Z}_q^{n\ell \times n}$ и LWE выборки $(G, \vec{b} = G\vec{s} + \vec{e} \bmod q)$.

Задание 4. На программирование. Взлом криптосистемы NTRU для малых параметров (5 баллов)

Криптосистема NTRU [1] на сегодняшний день является одним из вероятных кандидатов на стандартизацию пост-квантовых методов шифрования с открытым ключом. Взломать криптосистему можно с помощью алгоритмов редукции решеток. Ваша задача: запрограммировать простейшую атаку на NTRU для небольших параметров.

Для начала рассмотрим алгоритмы генерации ключей, шифрования и дешифрования в NTRU. Здесь будет представлен один из возможных вариантов NTRU, коих сейчас существует много.

Обозначим за $R = \mathbb{Z}[x]/(x^n - 1)$ - кольцо многочленов для некоторого положительного n, за $R_q = R/qR$ – фактор-кольцо по модулю некоторого q (в наших примерах q будет степенью двойки), $R_p = R/pR$ – фактор-кольцо по модулю простого $p = 3$. Иначе, в R_q лежат многочлены степени меньшей n с коэффициентами по модулю q (аналогично, R_p). Будем называть многочлен f тернарным, если все его коэффициенты лежат во множестве $\{-1, 0, 1\}$.

Функции генерации ключа KeyGen, шифрования Enc и дешифрования Dec работают следующим образом. Публичный параметр системы – целое положительное n, q – степень двойки, $p = 3$.

KeyGen(n).

1. Выбрать тернарный многочлен f, обратимый в R_q и в R_p. Обозначим $\tilde{f} = f^{-1} \bmod 3$.
2. Выбрать тернарный многочлен g.
3. Вычислить $h = 3g/f$ в R_q.
4. $pk = h$, $sk = (f, \tilde{f})$.

Enc($pk, m \in R_q$ с бинарными коэффициентами).

1. Выбрать r – тернарный многочлен в R_q.
2. $c = h \cdot r + m$ в R_q.

Dec(sk, c).

1. Вычислить $c' = c \cdot f$ в R_q
2. Вычислить $m' = c' \cdot \tilde{f}$ в R_p.

Убедимся в корректности схемы. В процедуре шифрования имеем

$$c' = h \cdot r \cdot f + m \cdot f = 3 \cdot g \cdot r + m \cdot f \text{ в } R_q.$$

Для модуля $q > |3 \cdot g \cdot r + m \cdot f|$, последнее выражение справедливо над $\mathbb{Z}$. Тогда второй шаг в процедуре дешифрования вычислит $(3 \cdot r \cdot g \cdot \tilde{f} + m \cdot f \cdot \tilde{f}) = m$ в R_p.

Атака на NTRU с помощью решеток. Рассмотрим атаку на секретный ключ криптосистемы NTRU. Заметим, что сравнение $hf = g$ в R_q можно переписать над целыми как $hf = g + kq$, для некоторого многочлена k. Таким образом, вектор (f, g) принадлежит решетке NTRU – решетке полного ранга $2n$, порожденной столбцами следующей матрицы

$$B_{\text{Ntru}} = \left(\begin{array}{c|c} rot(h) & q\mathbf{Id}_n \\ \hline \mathbf{Id}_n & \mathbf{0} \end{array}\right),$$

где $n \times n$ матрица $rot(h)$ содержит в i-ой строке вектор-коэффициентов многочлена $x^i \cdot h$ в R_q. Иными словами, матрица $rot(h)$ задает умножение на многочлен h в R_q. Заметим, что $B_{\text{Ntru}} \cdot (f, -k)^t = (g, f)^t$, то есть вектор (g, f) принадлежит решетке NTRU (^{t} означает знак транспонирования). Заметим также, что по теореме Минковкого мы ожидаем $\lambda_1(L(B_{\text{Ntru}})) \approx \sqrt{2n}\det(B_{\text{Ntru}})^{1/2n} = \sqrt{2n}q^{\frac{n}{2n}} = \sqrt{2nq}$. Если $\|(f, g)\| \ll \sqrt{2nq}$ (что верно по корректности криптосистемы), то мы можем восстановить (f, g), решив задачу unique SVP в решетке NTRU. Отметим, что в этой решетке также лежат n векторов вида $(x^i f, x^i g), i < n$, каждый их них длины $\|(f, g)\|$, и любой из них можно использовать для декодирования.

Задание: реализовать атаку на NTRU.

1. Со страницы курса скачать скрипт ntru.sage. В нем реализованы процедуры KeyGen,Enc,Dec.

2. Изменять нужно функцию attack(). А именно, в ней должна быть реализована функция, получающая на вход параметры n, q и произвольный открытый ключ криптосистемы. Функция должна построить базис решетки NTRU для $n = 19, q = 512$

3. Функция должна с помощью LLL алгоритма восстановить открытый ключ (или его ротацию) (f, g). Подтвердите корректность найденного ключа вызовом алгоритма дешифрования произвольного сообщения.

4. В итоге функция attack() должна выдавать секретный ключ и показывать корректности дешифрования с помощью найденного ключа.

5. При отправке выполненного задания, нужно переименовать файл в свою фамилию, оставив при этом расширение, например alisova.sage.

Список литературы

[1] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman, *NTRU: A ring-based public key cryptosystem* International Algorithmic Number Theory Symposium 1998