Е. Киршанова БФУ им. И.Канта

Контрольная работа

по дисциплине

Криптография на решетках

Время: 180 минут + 10 минут на скан и отправку
03.06.2024

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 **11:40**.

Задание	1	2	3	4
Баллы	/ 6	/ 5	/ 5	/ 5

Задание 1. Тривиальные задачки (1×6 баллов)

1 Пусть $B^\star$ – Грам-Шмидт базис векторов $\{\vec{b}_1, \ldots, \vec{b}_n\}$. Является ли $B^\star$ базисом решетки, порожденной $\{\vec{b}_1, \ldots, \vec{b}_n\}$?

2 Пусть решетка $L \subset \mathbb{Z}^2$ задана как

$$L = \{v \in \mathbb{Z}^2 \ : \ v_1 + v_2 = 0 \bmod 2\}$$

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

3 Положим, для целого $n \geq 1$ евклидова решетка L задана базисом $5\mathsf{Id}_n$. Опишите ранг решетки, все её последовательные минимумы, а также базис $\hat{L}$– решетки, дуальной к L.

4 Положим, даны две матрицы $B_1, B_2 \in \mathbb{Z}^{n \times n}$ ранга n. Как определить, порождают ли они одну и ту же решетку? (Вопрос требует алгоритма, а не только свойства.)

5 Пусть L' – подрешетка полного ранга решетки L (то есть ранги L и L' совпадают). Выберите все корректные утверждения.

A. $\det L'$ делит $\det L$

B. $\det L$ делит $\det L'$

C. $\lambda_1(L) \leq \lambda_1(L')$

D. $L' = L \iff \det L = \det L'$.

6 Верно ли, что решетка $\mathbb{Z}^2$ порождена базисом $B = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$? Ответ поясните.

Задание 2. Подрешетка в любой целой решетке (5 баллов)
Докажите, что для любой целочисленной решетки L полного ранга справедливо $\det(L) \cdot \mathbb{Z}^n \subseteq L$.

Задание 3. Решетки в теории чисел (5 баллов)
Докажите с помощью решетки ранга 2 следующий факт из теории чисел:

Для простого $p \equiv 1 \bmod 4$, существуют целые a, b такие, что $p = a^2 + b^2$.

Для этого, рассмотрите $\mathbb{Z}_p^\star$ и заметьте, что -1 – квадрат в $\mathbb{Z}_p^\star$. Используя существование i такого, что $i^2 \equiv -1 \bmod p$, постройте решетку ранга 2 с определителем p. Применяя к построенной решетке теорему Минковского, покажите, что в решетке найдется вектор, квадрат длины которого есть p.

Задание 4. На программирование. Взлом криптосистемы Меркля-Хэллмана (5 баллов)

Криптосистема Меркля-Хэллмана [1] была благополучно взломана Ади Шамиром с помощью решеток в работе [2]. Из-за этого долгие годы решетки считались лишь методами взлома, а не основой для конструкций безопасных криптопримитивов. Ваша задача состоит в реализации атаки Шамира.

Начнем с описания криптосистемы. Для формирования секретного ключа нам понадобится определение сверхвозрастающей последовательности.

Определение. Сверхвозрастаюшая последовательность – список целых положительных чисел $\mathbf{r} = (r_1, \ldots, r_n)$, таких, что

$$r_i > 2r_{i-1}, \quad 2 \leq i < n.$$

Из определения следует $r_k > r_{k_1} + \ldots + r_1$ для всех $2 \leq k \leq n$. Для сверхвозрастающей последовательности задача рюкзака решается тривиально: пусть дано $S \in \mathbb{Z}$, такое, что существует $\mathbf{b} \in \{0,1\}^n$, для которого выполняется

$$S = \sum_{i=1}^{n} b_i r_i.$$

Эффективный алгоритм решения задачи о рюкзаке:

Input:
Output:

$\mathbf{b} = \mathbf{0}$
for i **do** from n down to 1
  if $S \geq r_i$ **then**
    $b_i = 1$
    $S = S - r_i$

Функции генерации ключа KeyGen, шифрования Enc и дешифрования Dec работают следующим образом. Публичный параметр системы – целое положительное n.

KeyGen(n).

1. Сгенерировать сверхвозрастающую последовательность $\mathbf{r}$
2. Выбрать A, q, такие, что $q > r_n$ и $\gcd(A, q) = 1$.
3. Вычислить последовательность $M_i = Ar_i \bmod q$
4. $pk = \mathbf{M}$, $sk = (A^{-1} \bmod q, q, \mathbf{r})$.

Enc($pk, \mathsf{m} \in \{0,1\}^n$).

1. $c = \sum_{i=1}^{n} M_i \mathsf{m}_i \in \mathbb{Z}$

Dec(sk, c).

1. Вычислить $c' = c \cdot A^{-1} \bmod q$
2. С помощью эффективного алгоритма для задачи о рюкзаке, найти $\mathsf{m}' \in \{0,1\}$ для $c' \in \mathbb{Z}, \mathbf{r}$.

В корректности схемы вы можете убедиться самостоятельно. В безопасности убеждаться не смысла, так как сейчас мы увидим эффективный алгоритм дешифрования шифр-текста c без знания секретного ключа.

Атака Шамира. Шамир в [2] заметил, что из открытого ключа $\mathbf{M}$ и шифр-текста c можно сформировать решетку, порожденную **строками** следующей матрицы размера $(n+1) \times (n+1)$:

$$B = \begin{pmatrix} 2 & 0 & 0 & \dots & 0 & M_1 \\ 0 & 2 & 0 & \dots & 0 & M_2 \\ 0 & 0 & 2 & \dots & 0 & M_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 1 & 1 & \dots & 1 & c \end{pmatrix}$$

Заметьте, что если m – открытый текст для шифр-текста c (то есть $c = \sum_{i=1}^{n} M_i \mathsf{m}_i$), то в решетке $L(B)$ (порожденной строками B), лежит вектор $\mathbf{t} = (2\mathsf{m}_1 - 1, 2\mathsf{m}_2 - 1, 2\mathsf{m}_1 - 1, 2\mathsf{m}_n - 1, 0) \in \mathbb{Z}^{n+1}$. Для бинарного m, это короткий вектор в $L(B)$, который может быть (для большинства интересных параметров) найден с помощью алгоритма LLL.

Задание: реализовать атаку Шамира.

1. Со страницы курса скачать скрипт merkle_hellman.sage. В нем реализованы процедуры KeyGen,Enc, Dec. Они даны для ознакомления того, как были сгенерированы тесты. Изменять и вызывать их не понадобится.

2. Изменять нужно функцию attack(). А именно, в ней должна быть реализована атака Шамира. Входные и выходные данные описаны в начале тела функции.

3. Проверить корректность реализации можно с помощью команды

   sage -t merkle_hellman.sage

   Так будут проверены три теста, представленные в теле программы. Задание считается выполненным, если программа проходит все тесты.

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

Список литературы

[1] Ralph Merkle and Martin Hellman, *Hiding Information and Signatures in Trapdoor Knapsacks.* IEEE Trans. Information Theory. 1978

[2] Adi Shamir, *A Polynomial Time Algorithm for Breaking the Basic Merkle-Hellman Cryptosystem.* CRYPTO. 1982