Дополнительная лабораторная работа № 5

Взлом хэш-функции

1 Хэш-функция на решетках

На задаче SIS можно построить хэш-функцию следующим образом:

1. Для фиксированных $m > n > 1$ и $q > 1$, выберем матрицу $A \leftarrow (\mathbb{Z}_q^{n \times m})$
2. Хэш-функция $\mathcal{H}_A$ определяется отображением

$$\begin{aligned} \mathcal{H}_A : \{0,1\}^m &\to \mathbb{Z}_q^n \\ x &\mapsto Ax \bmod q \end{aligned}$$

Цель работы: отыскать коллизию для $\mathcal{H}_A$.

Заметим, что коллизией для $\mathcal{H}_A$ будет считаться любая пара бинарных векторов (x, x'), такая, что $x \neq x'$ и $Ax = Ax' \bmod q$. Из последнего равенства следует, что $A(x - x') = 0 \bmod q$, а значит, $x, x' \in L^\perp(A)$. Эту пару можно найти с помощью алгоритма редукции базиса $L^\perp(A)$.

2 Задание к лабораторной

Задача: для параметров $n = 12, m = 113, q = 37$, найти коллизию для хэш-функции $\mathcal{H}_A$. Пример реализации хэш-функции можно найти по адресу `https://crypto-kantiana.com/elena.kirshanova/teaching/lattices_2021/lab5.sage`

Код лабораторной должен вывести коллизию для $L^\perp(A)$. Алгоритм должен работать для случайной матрицы A.