Лабораторная работа № 3

Задача спрятанного числа

06.04.2021

1 Формулировка задачи

Задача "спрятанного числа" (англ. the Hidden Number Problem, HNP) была поставлена в статье [1] в связи со сторонними атаками на задачу Диффи-Хэллмана (ДХ). На сложности задачи ДХ основан популярный алгоритм генерации общего ключа: Алиса и Боб, обладая секретными a, b соответственно, обмениваются значениями g^a, g^b, формируя тем самым общий ключ $g^{a,b}$. Полагаем, что g–образующий мультипликативной группы $\mathbb{F}_p^\star$ для большого простого p. Задача ДХ говорит о том, что любой эффективный атакующий, зная g, g^a, g^b, не может вычислить g^{ab}. Что, если атакующий имеет доступ к некоторым битам g^{ab}? С учетом корявых реализаций этого важного протокола, вопрос не праздный [2], [3]. Этот вопрос мотивирует задачу HNP.

Определение 1. *Задача спрятанного числа. Зафиксируем простое p и целое положительное δ. Обозначим за $\mathcal{O}_\alpha(t)$–оракул, который выдает δ значимых бит числа $\alpha t \bmod p$:*

$$\mathcal{O}_\alpha(t) = \mathtt{MSB}_\delta(\alpha \cdot t \bmod p).$$

Задача состоит в вычислении α, имея доступ к $\mathcal{O}_\alpha(t)$.

Суть этой лабораторной состоит в реализации алгоритма, решающую задачу HNP. Отметим, что чем меньше δ, тем сильнее считается атака ($\delta = \lceil \log(p) \rceil$ делает задачу тривиальной).

Уточним определение `MSB`. Для атаки удобно думать о функции $\mathtt{MSB}_\delta(x)$ как о функции, возвращающей *любое* целое z, удовлетворяющее $|x - z| < p/2^\delta$. Такое определение будет удобно для анализа алгоритма, который мы рассмотрим ниже.

2 Решение задачи HNP

Основной результат Боне-Венкатесана [1] формулируется так: для $\delta = \lceil \sqrt{n} \rceil + \lceil \log n \rceil$ и $d = 2\sqrt{n}$ вызовов оракула $\mathcal{O}_\alpha(\cdot)$ задача HNP решается за детерминированное полиномиальное (от $\log p$) время.

Положим, мы выбрали d случайных значений $t_1, \ldots, t_d$ из $\mathbb{F}_p$ и запросили $\mathcal{O}_\alpha(t_i)$. Получили d значений $a_1, \ldots, a_d$, каждый из которых удовлетворяет

$$|\alpha t_i \bmod p - a_i| < p/2^\delta.$$

Построим решетку ранга $d+1$, порожденную столбцами

$$B = \begin{pmatrix} p & 0 & 0 & \ldots & 0 & t_1 \\ 0 & p & 0 & \ldots & 0 & t_2 \\ 0 & 0 & p & \ldots & 0 & t_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & p & t_d \\ 0 & 0 & 0 & \ldots & 0 & 1/p \end{pmatrix}$$

Заметим, что умножив последний столбец матрицы B на α и отняв необходимые кратные p с помощью остальных столбцов, мы получим вектор решетки

$$v = (r_1, \ldots, r_d, \alpha/p),$$

где $|r_i - a_i| < p/2^\delta$. Обозначим $u = (a_1, \ldots, a_d, 0)$. Этот вектор нам известен и $\|u - v\| \leq \sqrt{d+1}p/2^k$. Таким образом, пара $(L(B), u)$ формируют задачу ближайшего вектора. Боне-Венкатесана [1] доказывают, что это не просто задача ближайшего вектора, а уникального ближайшего вектора, которую, при указанных параметрах можно решить с помощью алгоритма Бабая (LLL).

3 Задание

Реализовать алгоритм, решающий задачу HNP для p порядка 2048 бит. Для реализации оракула можете использовать скрипт [4], а для нахождения ближайшего вектора можно использовать функцию babai (реализована в fpylll), либо метод вложения (см. лекцию про редукцию рюкзака к CVP).

Список литературы

[1] D. Boneh and R. Venkatesan. *Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes.* `https://link.springer.com/content/pdf/10.1007%2F3-540-68697-5_11.pdf`.

[2] Robert Merget, Marcus Brinkmann, Nimrod Aviram, Juraj Somorovsky and Johannes Mittmann, Jörg Schwenk *Raccoon Attack: Finding and Exploiting Most-Significant-Bit-Oracles in TLS-DH(E)* `https://eprint.iacr.org/2020/1151`

[3] `https://raccoon-attack.com/`

[4] `https://crypto-kantiana.com/elena.kirshanova/teaching/lattices_2021/tp3_oracle`