Лабораторная работа № 2

Задача спрятанного числа

02.03.2022, Дедлайн: 15.03.2022

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^{ab}. 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]. 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 $\alpha t \mod p$:*

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

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 $\mathrm{MSB}_\delta(x)$ 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 значений $a_1, \ldots, a_d$, каждый из которых удовлетворяет

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

Построим решетку ранга $d+1$, порожденную *столбцами*

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

Заметьте, во-первых, что матрица не целочисленная. Эту проблему мы далее решим. Во-вторых, умножив последний столбец матрицы B на α (который нам неизвестен) 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, кроме этого, $\|u - v\| \leq \sqrt{d+1} \cdot p/2^\delta$.

Таким образом, пара $(L(B), u)$ формирует задачу близкого вектора. Однако, с базисом, описанным выше, трудно оперировать на практике, так как он не является целочисленным. Для решения этой проблемы воспользуемся трюком, предложенным в [3]. Напомним, что мы имеем сравнения

$$\alpha t_i \equiv a_i + b_i \bmod p, \tag{1}$$

из которых нам известны t_i, b_i, неизвестны α и b_i, т.ч. $|b_i| < p/2^\delta$. Из сравнений (1), выполняется $\alpha \equiv t_1^{-1}(a_1 + b_i) \bmod p \equiv t_i^{-1}(a_i + b_i) \bmod p$, $\forall i$. Значит,

$$\begin{aligned} t_i \cdot t_1^{-1}(a_1 + b_1) &\equiv (a_i + b_i) \bmod p \iff \\ t_i \cdot t_1^{-1} b_1 &\equiv a_i - t_i \cdot t_1^{-1} a_1 + b_i \bmod p \end{aligned}$$

Полагая $\hat{t}_{i-1} := t_i \cdot t_1^{-1}$ для $i > 1$, а $\hat{a}_{i-1} := a_i - t_i \cdot t_1^{-1} a_1$, мы получаем новую инстанцию задачи HNP с неизвестным b_1 (вместо α). Рассмотрим теперь решетку, порожденную столбцами $\hat{B}$:

$$\hat{B} = \begin{pmatrix} p & 0 & 0 & \ldots & 0 & \hat{t}_1 \\ 0 & p & 0 & \ldots & 0 & \hat{t}_1 \\ 0 & 0 & p & \ldots & 0 & \hat{t}_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & p & \hat{t}_{d-1} \\ 0 & 0 & 0 & \ldots & 0 & 1 \end{pmatrix}.$$

Заметьте, что (известным нам) вектор $\hat{u} = (\hat{a}_1, \ldots, \hat{a}_{d-1}, \lceil p/2^\delta \rceil)$, отстает от вектора решетки $L(\hat{B})$ на вектор $(b_2, \ldots, b_d, \star)$, где $|\star| = p/2^\delta - b_1 < p/2^\delta$, а значит $(L(\hat{B}), \hat{u})$ формируют задачу нахождения близкого вектора.

3 Задание

Реализовать алгоритм, решающий задачу HNP для p порядка 512 бит. Для реализации оракула можете использовать скрипт [4] а для нахождения ближайшего вектора можно использовать функцию babai (реализована в fpylll). Вам нужно восстановить как значение b_i, так и α.

Список литературы

[1] D. Boneh, 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] M. R. Albrecht, Heninger. *On Bounded Distance Decoding with Predicate: Breaking the "Lattice Barrier" for the Hidden Number Problem* `https://eprint.iacr.org/2020/1540.pdf`

[4] `https://crypto-kantiana.com/elena.kirshanova/teaching/lattices_2022/tp2_oracle.sage`