Лабораторная работа № 4

NTRU Криптосистема

Дедлайн: 15.05.2023

Исторически, одним из первых предложенных постквантовых решений в области криптосистем является криптосистема NTRU, предложенная в 1996-м году Сильверманом, Хоффштейном и Пайпером в своей статье [3]. Оригинальная статья вводила так называемое NTRU предположение, состоящее в том, что нахождение решения уравнения $h = f/g \pmod{x^n - 1} \pmod{q}$ для простого q, n – степени двойки, где h известно, а неизвестные f и g малы относительно еквклидовой нормы, является вычислительно сложной задачей.

Есть множество вариантов NTRU: классический, упомянутый выше, HRSS, HPS, NTRU Prime [4]. В данной лабораторной работе мы используем HRSS подобный вариант NTRU. Процедура генерации ключей в нашей лабораторной выглядит следующим образом:

Algorithm 1 KeyGen

Input: Φ_d – многочлен степени d,
p – малое простое (обычно 3),
q – простое.

Output: $f, g \in \mathbb{Z}[x]/\Phi$ – секретный ключ (f – обратим),
$h \in \mathbb{Z}[x]/\Phi$ – открытый ключ.

1: $f, g \leftarrow^{\$} \{-p/2 \leqslant k < p/2\}$, где f обратим в $\mathbb{Z}[x]/\Phi$
2: Обратить $f \in \mathbb{Z}[x]/\Phi$ сначала по модулю p, затем по модулю q:

$$\mathbf{f} := \left((f^{-1} \pmod{p})^{-1} \pmod{q} \pmod{\Phi}\right)$$

3: $h := p \cdot g \cdot \mathbf{f} \bmod q \bmod \Phi$
4: **return** g, f, h

Алгоритм шифрования представлен ниже:

Algorithm 2 Encrypt

Input: Φ_d – многочлен степени d,
p – малое нечётное простое (обычно 3),
q – простое,
f, g – секретный ключ,
$m \in \mathbb{Z}[x]/\Phi$ – сообщение с коэффициентами $m_i \in \{-p/2 \leqslant k < p/2\}$

Output: c – зашифрованное сообщение.

1: $r \leftarrow^{\$} \{-p/2 \leqslant k < p/2\}$ – ослепляющий многочлен.
2: $c := h \cdot r + m \pmod{q}$
3: **return** c

Расшифровать сообщение можно при помощи следующего алгоритма:

Algorithm 3 Decrypt

Input: Φ_d – многочлен степени d,
p – малое простое (обычно 3),
q – простое,
f, g – секретный ключ,
$c \in \mathbb{Z}[x]/\Phi$ – зашифрованное сообщение.

Output: m – дешифрованное сообщение

1: $a := (e \cdot f \pmod q) \pmod p$
2: **return** $m = \left(a \cdot (f^{-1} \pmod p)\right) \pmod p$

Доказать корректность несложно: по модулю q имеем $e = (p \cdot g \cdot \mathbf{f}) \cdot r + m$. Тогда $a = e \cdot f = p \cdot g \cdot r + m \cdot f$. Если взять a по модулю p и в результате операций зашифрования и расшифрования не произошло переполнения, то останется $b = m \cdot f \pmod p$. Умножим b на $f^{-1} \pmod p$ и получим $m \pmod p$. Заметьте, что хранить коэффициенты всех элементов кольца многочленов по модулю p или q нужно в промежутках $\{-p/2 \leqslant k < p/2\}$ и $\{-q/2 \leqslant k < q/2\}$ соответственно.

В 1999-м году Копперсмитом [1] была предложена первая атака при помощи решёток на криптосистему NTRU. Оригинальная атака опиралась на особый вид многочлена $\Phi = x^{2^n} - 1$, но мы приведём более общую атаку. Рассмотрим алгебраическую решётку:

$$B = \begin{pmatrix} q & 0 \\ h & 1 \end{pmatrix}, \tag{1}$$

где, помимо векторов $(q, 0)$ и $(h, 1)$ из $(\mathbb{Z}[x]/\Phi)^2$ лежат также их линейные комбинации с коэффициентами из $\mathbb{Z}[x]/\Phi$, если Φ – это циклотомический многочлен. В этом случае $\mathbb{Z}[x]/\Phi$ - это кольцо целых числового поля $\mathbb{Q}[x]/\Phi$.

В ней же лежит вектор с коэффициентами (g, f) относительно базиса B. Его координатами являются $(g, f) \cdot B = (qg + g, f)$. Так как вместе с вектором решётки вида $(qt + x, y)$ в ней же лежит и вектор вида (x, y) (подумайте, почему), то в решётке, порождённой B лежит и вектор (g, f). Он является аномально коротким и может быть найден при помощи BKZ алгоритма.

Но как редуцировать алгебраические решётки? На данный момент нам неизвестно о существовании специализированных эффективных алгоритмов редукции алгебраических решёток. Поэтому нам придётся погрузить решётку в поле $\mathbb{Q}$. Пусть $K = \mathbb{Q}[x]/\Phi$ циклотомическое поле, заданное циклотомическим многочленом Φ. Тогда K получается присоединением примитивного корня ζ_f степени f из единицы [1]. Коэффициентным вложением элемента $k = \sum_{0 \leqslant i < d} k_i \cdot \zeta^i \in K$ является вектор размерности d, состоящий из чисел k_i. Вложением вектора (x, y) является решётка над полем $\mathbb{Q}$ размерности d задаваемая базисом, состоящим из d векторов длины $2d$: $\zeta^i \cdot (x, y)$ для $0 \leqslant i < d$. Базис вложения решётки является базисом, состоящим из вложений всех исходных векторов алгебраической решётки.

Пример: пусть K – шестое циклотомическое поле ($\Phi = x^2 - x + 1$). Тогда $d = 2$ и мы имеем $\zeta_6^2 - \zeta_6 + 1 = 0$. Пусть:

$$B = \begin{pmatrix} 7 & 0 \\ 1 \cdot \zeta_6 + 1 & 1 \end{pmatrix}. \tag{2}$$

[1] Число f называют кондуктором поля. Степень d поля и кондуктор соотносятся через функцию Эйлера: $d = \phi(f)$

Тогда вложением элемента $x + y \cdot \zeta_6 \in K$ в $\mathbb{Q}$ будет решёлка ранга 2, порождённая векторами (x, y) и $(\zeta_6 x, \zeta_6 y)$, а вложением B будет:

$$\begin{pmatrix} 7 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ -1 & 2 & 0 & 1 \end{pmatrix}$$

Как и в случае с RSA, неправильно подобранные параметры могут привести к слабой защищённости криптосистемы. В случае криптосистем на решетках, как правило, чем больше размерность поля, тем защищённей система. Однако непропорционально большой q, суперполиномиально зависящий от d тоже сильно бьёт по защищенности системы [2]. Данная атака основана на наблюдении, что нам необязательно находить секретный ключ: достаточно найти достаточно короткий вектор (g', f') в алгебраической подрешётке, порождённой (g, f) и использовать его в качестве ключа.

Задание

В данной лабораторной работе вам будет дан 432-й циклотомический многочлен $x^{144} - x^{72} + 1$ степени 144, простые $q \approx 2^{13}$, $p = 3$, публичный ключ h и зашифрованное сообщение e. Вам нужно найти короткий вектор решётки (g', f') из плотной подрешётки, порождённой (g, f) и дешифровать с его помощью сообщение. Для этого вам следует построить базис решётки B, вложить его в $\mathbb{Q}$ и вызвать на нём LLL. После этого следует вызвать BKZ алгоритм с возрастающим параметром размера блока β [2]. Примеры составлены так, что при $\beta \approx 40$ такой вектор должен отыскаться. В сообщении содержится название музыкальной группы, поэтому корректность атаки можно проверить наглядным образом. Заметьте, что секретный ключ (g', f') будет найден с точностью до знака и умножения на степень ζ_{432}^i, где $i < 144$, поэтому стоит сгенерировать 288 ключей и проверить, какой из них подойдёт.

Параметры системы для каждой группы представлены в файлах с именем одного из студентов группы `https://crypto-kantiana.com/elena.kirshanova/teaching/lattices_2023/`. Код, использующийся для генерации параметров, лежит тут `https://crypto-kantiana.com/elena.kirshanova/teaching/lattices_2023/labntru/labgen.sage`

Список литературы

[1] Don Coppersmith and Adi Shamir. Lattice attacks on NTRU. In *Advances in Cryptology—EUROCRYPT'97*, pages 52–61. Springer, 1997.

[2] Léo Ducas and Wessel van Woerden. NTRU fatigue: How stretched is overstretched? Cryptology ePrint Archive, Report 2021/999, 2021. `https://ia.cr/2021/999`.

[3] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, *ANTS-III*, pages 267–288, 1998.

[4] John M Schanck. A comparison of NTRU variants, 2018. `https://eprint.iacr.org/2018/1174`.

[2] Мы вызывали, начиная с $\beta = 4$ с шагом в 2.