Министерство науки и высшего образования Российской Федерации ФГАОУ ВО «Балтийский федеральный университет имени Иммануила Канта»

УТВЕРЖДАЮ
ректор БФУ им. И. Канта
_____ А.А. Фёдоров
«__»_____ 2021 года

Отчет
о научно-исследовательской работе _____ этап
“Алгоритмы нахождения короткого вектора в алгебраических решётках”
(договор на выполнение НИР № 2165 от 8 октября 2021 года)

Исполнитель _____

Согласовано:
Проректор по научной работе
_____ М.В. Дёмин

Руководитель проекта
_____ Е.А. Киршанова

Калининград
2021

Практическое измерение зависимости параметра размера блока при вызове BKZ алгоритма от размерности n решётки, модуля q и индекса r подрешётки

А.С. Каренин

13 декабря 2021 г.

1 Результаты вычислительных экспериментов

1.1 Гипотеза

Пусть $\mathcal{L}$ - Z-решётка[1], также являющаяся NTRU-решёткой, q - простое число, n - степень некоторого числового поля $\mathcal{K}$, r - натуральное, делящее n. Обозначим за B матрицу $(b_1, ..., b_n, b_{n+1}, ..., b_{2n})^T$,[2] столбцами которой являются базисные векторы. Тогда для NTRU решёток она примет вид:

$$\boldsymbol{A} = \begin{pmatrix} \boldsymbol{I}_n & \boldsymbol{0}_n \\ rot(\boldsymbol{h}) & q \cdot \boldsymbol{I}_n \end{pmatrix} \tag{1}$$

В статье [KF17] был предложен метод атаки с использованием подколец, заключающийся в следующем: сначала выберем $r >= 1$[3] вычеркнем из нижней половины матрицы все строки, не сравнимые с 0 по модулю r. После этого (если $r \neq 0$), то нижней правой части матрицы, соответствовавшей $q \cdot \boldsymbol{I}_n$ у нас возникнут нулевые столбцы.[4] Так как над этим блоком матрицы лежит нулевой блок, такие столбцы можно исключить из рассмотрения и вычеркнуть. После этого из матрицы можно вычеркнуть последние $n + n/r - D$ столбцов и строк для некоторого $D \in \mathbb{N}$, таким образом получив матрицу B'. После этого проводится BKZ редукция и последующий подъём решения в исходную решётку. Необходимым условием для работы атаки является большой модуль $q \geqslant O\left(n^{2.483}\right)$ [DvW21]. Если q удовлетворяет этому неравенству, то говорят, что имеет место растянутый режим (overstretched regime).

Целью настоящего вычислительного эксперимента было поставлено определение соотношения параметра β вызова BKZ алгоритма и параметра D размерности матрицы B', полученной из матрицы B вычёркиванием строк и столбцов с индексами $i \in Ind$ и проверка гипотезы о том, что по мере роста числа исключённых из матрицы B строк и столбцов требуемое значения параметра β BKZ алгоритма для успешного отыскания короткого вектора решётки также почти монотонно возрастает.

1.2 Постановка эксперимента

Для эксперимента были выбраны 24 различные решётки[5] размерности $2n = 192$. Модулю q было поставлено значение 751, что соответствует растянутому режиму для данно-

[1] E: $\mathbb{Z}$-решетка
[2] троеточие оформляется через ...
[3] $\geq$
[4] E: перечитайте предложение, у меня оно не компилируется
[5] NTRU решетки

го n.[6] В качестве числа D[7] оставленных измерений были взяты значения $192, 187, 182, 177, 172, 162, 157$. Методика эксперимента заключается в следующем: в рамках вычислений параметр r полагается равным 1.
Для каждого из рассматриваемых D на построенной матрице B' последовательно вызывался BKZ алгоритм начиная с параметра $\beta = 2$ и повышая его на 1 по прошествии 20 туров алгоритма. Минимальный параметр β для которого удалось успешно найти требуемый вектор запоминался, и по прошествии всех экспериментов высчитывалось среднее арифметическое этих значений. При этом редукция считалась успешной вне зависимости от того, произошло ли событие отыскания ротации ключа (SKR), или событие нахождения плотной подрешётки (DSD).

Программный код эксперимента доступен по запросу на почтовый ящик ASKarenin@stud.kantiana.ru.

1.3 Результаты

В результате проведения эксперимента были получены следующие зависимости среднего арифметического β достаточного для успешной редукции подрешётки размерности D решётки $\mathcal{L}$:

D	β
192	6.5
187	9
182	9.08
177	9.708
172	9.83
167	9.75
162	11.0833
157	11.958
152	14.75

Полученные данные свидетельствуют о почти монотонном возрастании параметра β при уменьшении числа D измерений матрицы B'. График зависимости приведён на рисунке ниже:

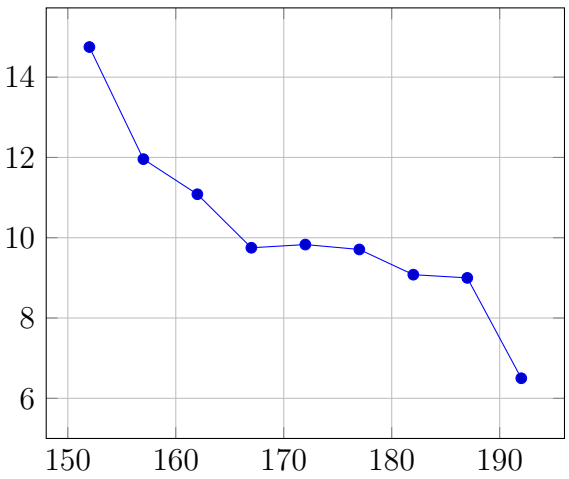

Рис. 1. Сравнение зависимости β (ось абсцисс) от числа измерений D.

[6] n
[7] поясните, что $D = n - r$

2 Выводы

Данные, полученные в результате эксперимента не противоречат рассуждениям, проведённым в [KF17] [DvW21]: действительно, в этих статьях сравнивается эффективность атаки методом подполей и атаки методом подколец, но они не сравниваются экспериментально с атакой на полную решётку.

Из полученных результатов можно сделать вывод, что данный алгоритм атаки не даёт преимущества во времени выполнения перед атакой на полную решётку ($D = 2n$) по крайней мере для размерностей не превышающих рассмотренную в эксперименте и при вычёркивании последних строк матрицы.

Дальнейшее развитие данного эксперимента может осуществляться двумя путями:

- Экстенсивный путь: достигается увеличением размерности при параллельной подгонке параметра q к значениям, лежащим в непосредственной близости от точки усталости (fatigue point) NTRU решётки, нынешнюю оценку которой можно найти в [DvW21];
- Интенсивный путь: достигается иными алгоритмами вычёркивания строк. Например, при вычёркивании всех не сравнимых с 0 по модулю r строк и некоторых соответствующих им столбцов, можно получить матрицу, задающую базис подрешётки исходной решётки. Интересным вопросом остаётся возможность уменьшения темпов роста β путём более тонкого анализа строк - кандидатов на вычёркивание.

Список литературы

[DvW21] Léo Ducas and Wessel van Woerden. Ntru fatigue: How stretched is overstretched? Cryptology ePrint Archive, Report 2021/999, 2021. `https://ia.cr/2021/999`.

[KF17] Paul Kirchner and Pierre-Alain Fouque. Revisiting lattice attacks on overstretched ntru parameters. pages 3–26, 04 2017.