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 решетках”
(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

6 апреля 2022 г.

1 Введение

Пусть $\boldsymbol{h} = \boldsymbol{g}/\boldsymbol{f}$. А матрица

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

2 Вопрос 1: Какова ожидаемая длина $(\boldsymbol{g}/\boldsymbol{f} \cdot N_{K/L}(\boldsymbol{f}), N_{K/L}(\boldsymbol{g}))$?

Мы знаем, что для решётки $\mathcal{L}(\boldsymbol{A})$ с вероятностью $1 - \epsilon$:

$$||\boldsymbol{g}/\boldsymbol{f} \cdot N_{K/L}(\boldsymbol{f})||_{op} \leqslant \sigma/s \cdot \left(s\sqrt{2\log(6n/\epsilon)/\pi}\right)^{|H|} \tag{2}$$

$$||N_{K/L}(\boldsymbol{f})||_{op} \leqslant \left(s\sqrt{2\log(6n/\epsilon)/\pi}\right)^{|H|} \tag{3}$$

где s - параметр Гауссова распределения, а $H = Gal(K/L)$. Операторная норма ограничивает сверху евклидову норму как $||\boldsymbol{v}|| \leqslant \sqrt{n}||\boldsymbol{v}||_{op}$ ввиду того, что она является наибольшей координатой вектора [DvW21], а он в свою очередь не длинее вектора "забитого"во всех своих координатах этим максимальным коэффициентом. Тогда существует такой $\boldsymbol{x} \in \mathbb{Z}^{2n}$, что

$$||\boldsymbol{A}\boldsymbol{x}|| \leqslant \sqrt{n(1+\sigma^2/s^2)}\left(s\sqrt{2\ln(6n/\epsilon)/\pi}\right)^{n/m}$$

с вероятностью не менее $1-\epsilon$. (Theorem 3 из [KF17]).

Набросок доказательства: Пусть

$$q\boldsymbol{y} + hN_{K/L}(f) = gN_{K/L}(f)/f$$

обозначим тогда

$$\boldsymbol{x} = \begin{pmatrix} \boldsymbol{y} \\ \boldsymbol{N_{K/L}(f)} \end{pmatrix}.$$

Умножим:

$$\boldsymbol{Ax} = \begin{pmatrix} \boldsymbol{N_{K/L}(f)} & \boldsymbol{y} \end{pmatrix} \begin{pmatrix} \boldsymbol{I}_n & rot(\boldsymbol{h}) \\ \boldsymbol{0} & q\boldsymbol{I}_n \end{pmatrix} \cdot = \begin{pmatrix} \boldsymbol{N_{(K/L)}(f)}, & q\boldsymbol{y} + \boldsymbol{h} \cdot N_{K/l}(f) \end{pmatrix}$$

Тогда:

$$\boldsymbol{xA} \equiv \begin{pmatrix} \boldsymbol{gN_{K/l}(f)/f} \\ \boldsymbol{N_{(K/L)}(f)}^T \end{pmatrix}$$

Операторная норма является инвариантом относительно автроморфизмов группы Галуа $Gal(K/L)$ и обладает свойством субмультипликативности, поэтому с вероятностью $1-\epsilon$:

$$||N_{K/L}(\boldsymbol{f})||_{op} \leqslant s\sqrt{2\ln(6n/\epsilon)/\pi}$$

Это так ввиду того, что:

$$\prod_{\sigma \in H} ||\sigma(x)||_{op} = ||\sigma(x)||_{op}^{|H|} = ||x||_{op}^{|H|}$$

с вероятностью $1-\epsilon$. Также:

$$||\boldsymbol{f} \cdot N_{K/L}(\boldsymbol{g})/\boldsymbol{g}||_{op} \leqslant \sigma/s \cdot ||N_{K/L}(\boldsymbol{f})||_{op} \leqslant \sigma/s \cdot s\sqrt{2\ln(6n/\epsilon)/\pi}$$

Ввиду ортогональности частей вектороа x имеем:

$$||\boldsymbol{xA}||_{op} = ||N_{K/L}(\boldsymbol{f})||_{op}^2 + ||\boldsymbol{f} \cdot N_{K/L}(\boldsymbol{g})/\boldsymbol{g}||_{op}^2$$

3 Вопрос 2: Проекция

3.1 Вопрос 2.1: Как работает проекция?

Пусть вектор v принадлежит решётке $\mathcal{L}(\boldsymbol{A}_{N_{K/L}})$, где

$$\boldsymbol{A}_{N_{K/L}} = \begin{pmatrix} \boldsymbol{I}_n & rot(N_{K/l}(\boldsymbol{h})) \\ \boldsymbol{0}_n & q \cdot \boldsymbol{I}_n \end{pmatrix} = \begin{pmatrix} \boldsymbol{I}_n & rot\left(\boldsymbol{\alpha} \cdot \boldsymbol{h}\right) \\ \boldsymbol{0}_n & q \cdot \boldsymbol{I}_n \end{pmatrix} = \begin{pmatrix} \boldsymbol{I}_n & \boldsymbol{\alpha} \cdot rot(\boldsymbol{h}) \\ \boldsymbol{0}_n & q \cdot \boldsymbol{I}_n \end{pmatrix}.$$

Тогда он принадлежит и решётке, порожденной базисом:

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

Обозначим:

$$\boldsymbol{B} = \begin{pmatrix} \boldsymbol{I}_n & (\boldsymbol{\alpha} \cdot \boldsymbol{I}_n - \boldsymbol{I}_n) \cdot rot(\boldsymbol{h}) \\ \boldsymbol{0}_n & \boldsymbol{I}_n \end{pmatrix}.$$

Заметим, что $\det \boldsymbol{B} = 1$ и применим к $\boldsymbol{A}_{N_{K/L}}$ преобразование $\boldsymbol{B}^{-1}$:

$$\boldsymbol{A}_{N_{K/L}} \cdot \boldsymbol{B}^{-1} = \begin{pmatrix} \boldsymbol{I}_n & rot(\boldsymbol{h}) \\ \boldsymbol{0}_n & \boldsymbol{I}_n \end{pmatrix}.$$

С другой стороны, если $r = [K : L]$, то все координаты v_i такие, что $i \neq 0 \ (mod\ r), i < n$ равны 0, а сам вектор v в базисе $\boldsymbol{A}_{N_{K/L}}$ записывается, как: $\boldsymbol{v} = (v_0, 0, ..., 0, v_r, 0, ..., 0, ..., v_{n-r-1}, 0, ..., 0, v_n, v_{n+1}, ..., v_{2n-1})$ по свойствам нормы $N_{K/L}$. Но тогда и в базисе $\boldsymbol{A}_{N_{K/L}} \cdot \boldsymbol{B}^{-1}$ его соответствующие i-е координаты будут нулевыми, так как левая верхняя часть матрицы $\boldsymbol{A}_{N_{K/L}} \cdot \boldsymbol{B}^{-1}$ такой же, как и у $\boldsymbol{A}_{N_{K/L}}$. Из этого следует, что можно просто вычеркнуть из базиса $\boldsymbol{A}$ такие i-е векторы и в порождённой такой матрицей $\boldsymbol{A}'$ решётке будет лежать каждый вектор из решётки $\boldsymbol{A}_{N_{K/L}}$. Это наблюдение позволяет нам вычёркивать из $rot(\boldsymbol{h})$ все строки, пронумерованные с нуля и не кратные r.

Теперь, когда мы вычеркнули нули из $rot(\boldsymbol{h})$, можно рассматривать вместо векторов $v = (v_0, v_1, ..., v_d, v_{d+1}, ..., v_{n+n/r})$ проецированные векторы $v_{proj} = (v_0, v_1, ..., v_d, 0, ..., 0)$. Очевидно, что решётка $\mathcal{L}'_{proj}$, порождаемая такими v_{proj}, это подрешётка решётки $\mathcal{L}'$ полученная из последней вычёркиванием последних $n - d$ строк, являющихся базисными векторами. Этот шаг помогает нам избавиться ещё от $n - d$ базисных векторов, а, значит, и измерений, но ценой того является алгебраическая структура. Отдельно отметим, что, вычеркнув последние $n - d$ строк, мы можем вычеркнуть и последние $n - d$ столбцов, спроицировав всю решётку ортогонально к оставшимся, что в итоге приведёт нас к матрице $\mathcal{L}'_{proj}$ размерности $(\frac{n}{r} + d) \times (\frac{n}{r} + d)$. После нахождения кратчайшего вектора, можно вновь подняться обратно в исходную решётку при помощи Babai nearest plane алгоритма или поднятие с уравнением нормы.

Отличие атаки подкольцом от атаки подполем заключается в том, что в подкольце мы используем ротацию $rot(\boldsymbol{h})$ открытого ключа, а не его нормы.

Докажем (4). BKZ возвращает вектор длиной не более $\beta^{d/\beta} \cdot Vol(\mathcal{L})^{1/d}$, но будем считать, что длина последнего есть $\sqrt{d}Vol(\mathcal{L})^{1/d}$. С другой стороны норма этого вектора дожна быть меньше $\sqrt{n}B$, где d-размерность решётки. Имеем:

$$\log(\beta)/\beta = 1/d \cdot \log(\frac{\sqrt{n}Vol(\mathcal{L})^{1/d}}{\sqrt{n}/B})$$

Это уравнение корректно, так как нам достаточно найти вектор $v : ||v|| \leqslant \gamma \cdot Vol(\mathcal{L})^{1/d}$ приравняем это к длине $\sqrt{d}Vol(\mathcal{L})^{1/d}$ вектора, возвращаемого BKZ и помня, что $\gamma = \frac{\sqrt{d}Vol(\mathcal{L})^{1/d}}{\sqrt{n}B}$ (так как γ есть апроксимационный фактор) получим:

$$\gamma = \beta^{d/\beta},$$

откуда и следует уравнение.

В итоге при overstretched q мы получаем слишком короткий вектор, чтобы он был случайным.

3.2 Вопрос 2.2: Оптимальный выбор размерности подрешётки.

Количество $n' + d$ строк и колонок, которые мы оставляем в атаке подполем, а также параметр β удовлетворяют следующим соотношениям:

$$n' + d \geqslant \frac{n' \log q + 1}{(\log q/B)} \frac{\beta}{\log \beta} = \frac{2n' \log q}{(\log q/B)^2} \tag{4}$$

где $r = n/n'$. В случае с подкольцом эти соотношения принимают следующий вид:

$$n' + d \geqslant \frac{n' \log q + 1}{(\log q\sqrt{r}/(\sqrt{2r+2}B + \sqrt{r}))} \frac{\beta}{\log \beta} = \frac{2n' \log q}{\left(\log\left(\sqrt{2r}q/(\sqrt{r+1}B)\right)\right)^2} \tag{5}$$

Это происходит ввиду того, что $B^2_{subfield}/\left(B^{proj}_{subring}\right)^2 \approx \frac{2r}{r+1}$.

Подставим в (5) $q = n^\alpha$ и $B = ||N_{K/L}(f)|| \approx ||f||^r n^{r/2} = ((2D+1)n)^{r/2}$, где D - параметр генерации f такой, что в f ровно $2D+1$ ненулевых координат, и избавимся от 1 в числителе вместе с $\sqrt{r}$ в подзнаменателе знаменателя в виду их пренебрежительной малости, после чего получим:

$$\frac{\beta}{\log \beta} \approx \frac{\alpha \cdot n \log n}{\left(r\left(\alpha \log n - \log\left(\sqrt{2r+2}\left[(2D+1)n\right]^{r/2}\right)\right)\right)^2}.$$

Для успеха атаки нужно, чтобы длина $\beta^{2n'/\beta}\lambda_1(\mathcal{L})$ была меньше, чем q, где n' является размерностью подрешётки, а в качестве $\lambda_1(\mathcal{L})$ можно взять $||(N_{K/L}(f), h \cdot N_{K/L}(f))||$. Выбор q можно попробовать объяснить органичениями по бесконечной норме, которая должна быть ограничена сверху $q/2$ для успешного декодирования [May99].

Для ответа на вопрос о размерности подрешётки достаточно предоставить критерии выбора $r = [K : L]$ и d - количество векторов в нижней полуматрице A', которое мы оставляем при составлении матрицы $\boldsymbol{A}_{proj}$.

При увеличении r увеличивается длина $\sigma/s \cdot s\sqrt{2\ln(6n/\epsilon)/\pi}$. Когда она становится больше $\sqrt{n} \cdot q$ наши шансы отыскать короткий вектор падают. Параметр d выбирается как $n/r \cdot \frac{\log(q^2)}{\log(q/B)}$.

Наши вычисления: приравняем апроксимационный фактор $\gamma = \frac{\sqrt{d} \cdot Vol\mathcal{L}^{1/dim}}{\sqrt{d} \cdot B}$, который мы бы хотели увидеть на практике к апроксимационному фактору, который достигается BKZ алгоритмом с размером блока β, вызванным на решётке размерности d, а именно $2^{d \cdot \log(\beta)/\beta}$:

$$\frac{\sqrt{d} \cdot Vol\mathcal{L}^{1/d}}{\sqrt{d} \cdot B} = 2^{d \cdot \log(\beta)/\beta} \tag{6}$$

Пусть $\delta = \sqrt{1 + \sigma^2/s^2}$, а $\xi = \left(s\sqrt{2\ln(6n/\epsilon)/\pi}\right)$, тогда:

$$\log(\sqrt{q}/\delta) - \log(\xi^r) = d \cdot \log(\beta)/\beta$$

Пусть мы проводим только редукцию f-части, тогда $d = n/r + n = n(r + 1/r)$ и тогда:

$$\frac{\log \beta}{\beta} = \frac{\log(\sqrt{q}/\delta) - r \cdot \log(\xi)}{n(r + 1/r)}$$

Для нахождения локального минимума $\frac{\log \beta}{\beta}$, а, значит, и локального максимума β возьмём производную и приравняем к нулю:

$$\frac{1}{n}\left(\log(\sqrt{q}/\delta) \cdot \frac{1}{(r+1)^2} - \log(\xi) \cdot \frac{r(r+2)}{(r+1)^2}\right) = 0.$$

Решением этого уравнения является:

$$\frac{\log(\sqrt{q}/\delta)}{\log(\xi)} = r(r+2). \tag{7}$$

4 Вопрос 3: Условия работы атаки.

Можно [DvW21] рассматривать два типа событий, которые могут возникнуть в процессе работы BKZ-редукции: SKR (secret key recovery) и DSD (dense sublattice recovery). Суть SKR заключается в том, что в очередном раунде в одной из строк базиса, с которым работает BKZ, появляется секретный ключ. DSD же происходит, когда в одной из строк базиса появляется вектор из плотной решётки $\mathcal{L}^{g,h}$. Обозначим:

$$\mathbb{E}[\lambda_1(\mathcal{L})] = \mathrm{gh}(\mathcal{L}) = \left(\frac{\mathrm{Vol}(\mathcal{L})}{\mathrm{Vol}(\mathcal{B}_1)}\right)^{1/d} \approx \sqrt{d/(2\pi e)} \cdot \mathrm{Vol}(\mathcal{L})^{1/d}$$

Отдельно обозначим $\mathrm{gh}(d) = \sqrt{d/(2\pi e)}$ и:

$$\alpha_\beta = \mathrm{gh}(\beta)^{2/(\beta-1)} \tag{8}$$

Теперь рассмотрим при каких условиях происходят события SKR и DSD. Для этого нам понадобится эвристика, объясняющая как выглядит профиль длинн Грама-Шмидта q-арных решёток после BKZ-редукции.

Определение: базис $\boldsymbol{B} = [\boldsymbol{b}_0, ..., \boldsymbol{b}_{d-1}]$ называется BKZ-редуцированным, если:

$$\forall \kappa \in \{0, ..., d-1\} : ||b_k^*|| = \lambda_1(\mathcal{L}_{\kappa:min(\kappa+\beta,d)}) \tag{9}$$

ZGSA: пусть нам дана решётка $\mathcal{L}$ размерности $2n \times 2n$ над $\mathbb{Z}$. Тогда профиль длин Грама-Шмидта после BKZ редукции будет выглядеть следующим образом:

$$||b_i^*|| = \begin{cases} q & , i \leqslant n+m \\ \sqrt{q} \cdot \alpha_\beta^{2n-1-2i} & m+n < i < n+m-1 \\ 1 & , \end{cases} \tag{10}$$

Где $m = 1/2 + \frac{\log q}{2\log(\alpha_\beta)}$.

Эта эвристика корректна в том смысле, что $\prod_{i=0}^{2n-1} ||b_i^*|| = q^n$. Индекс m здесь выбран таким образом, чтобы $\sqrt{q} \cdot \alpha_\beta^{2n-1-2(n+m-1)}$ был равен 1, для того чтобы график профилей не имел больших разрывов.

SKR эвристика: пусть $\mathcal{L}$ - решётка размерности d имеющая вектор v нормы $\ll \mathrm{gh}(\mathcal{L})$. Тогда по ZGSA имеем:

$$\sqrt{\beta/d} \cdot ||v|| < \alpha_\beta^{(2\beta-d-1)} \cdot \mathrm{Vol}(\mathcal{L})^{1/d}, \tag{11}$$

где левая часть это корень квадратный из длины проекции v (из всех d измерений, мы оставляем только β, поэтому её квадрат становится в среднем в d/β раз меньше),а правая часть - длина $||b_{d-\beta}^*||$.

Пусть k - количество q-векторов, не затронутых BKZ-редукцией. В асимптотике при $q = \Theta(n^{\mathcal{Q}})$, $||v|| = ||(f,g)|| = \Theta(n^{\mathcal{S}})$ и $\beta = (\mathcal{B} + o(1))n$ имеем:

$$k = \min\left((2\sqrt{\mathcal{BQ} - 1})n, n\right), \tag{12}$$

Причём $(2\sqrt{\mathcal{BQ} - 1})n < n$ при $S < 1$, соответственно мы можем вызывать BKZ-редукцию на подрешётке $\mathcal{L}_{[n-k:2n)}$. Тогда SKR событие происходит, когда:

$$\mathcal{B}_{SKR} = \frac{2}{\mathcal{Q} + 2 - 2\mathcal{S}}, S \geqslant 1 \tag{13}$$

$$\mathcal{B}_{SKR} = \frac{2}{(\mathcal{Q} + 1 - \mathcal{S})^2}, S < 1 \tag{14}$$

Теперь рассмотрим ситуацию, когда происходит DSD событие (claim 3.5 из [DvW21]).

DSD эвристика: Событие DSD для $\beta = \mathcal{B}n$ и параметров $q = \Theta(n^{\mathcal{Q}})$, $||v|| = ||(f,g)|| = \Theta(n^{\mathcal{S}})$ происходит когда:

$$\mathcal{B}_{DSD} = \frac{8\mathcal{S}}{\mathcal{Q}^2 + 1} + o(1). \tag{15}$$

Для тернарных секретов $\mathcal{S} = 1/2$. Количество k оставляемых векторов следует взять за $\mathcal{K}n = \frac{4\mathcal{S}n}{\mathcal{Q}^2+1}$.

Докажем это утверждение.

Как было показано ранее, мы можем рассматривать подрешётку размерности $n + n/r$, где $r = [K : L]$ для числовых полей K и L. По лемме Патаки Турала мы имеем ограничение сверху на объем решётки как произведение $\dim \mathcal{L}$ норм $||b_i^*||$ BKZ профиля, а именно последних n/r, из которых только первые $m-1$ являются неединичными.

При спуске в подрешётку норма кратчайшего вектора изменяется с $||f||$ до $||f||^r \cdot \sqrt{n} \approx n^{sr+1/2}$. Тогда

$$\prod_{i=n}^{n+m-2} \sqrt{q} \cdot \alpha_\beta^{2n-1-2i} = q^{\frac{m-1}{2}} \cdot \alpha_\beta^{-(m-1)^2} \approx q^{\frac{m-1}{2}} \cdot \alpha_\beta^{m(d-m-2n)/2} \tag{16}$$

Так как размерность d решётки равна $n + n/r$, параметр $m \approx QBn/2$, а $\alpha_\beta = (Bn)^{1/Bn}$ в асимптотике, то перепишем это неравенство как

$$n^{r/2} \cdot n^{Sn} < n^{\frac{Q^2Bn}{8} + \frac{Q \cdot d}{4} - \frac{Qn}{2}} \tag{17}$$

Тогда $r/2 + Sn < \frac{Q^2Bn}{8} + \frac{Q \cdot d}{4} - \frac{Qn}{2}$

$$\frac{Q^2Bn}{8} > Sn + \frac{r}{2} + \frac{Qn}{4} - \frac{Q}{4}$$
$$B > \frac{8S}{Q^2} + \frac{2}{Q} - \frac{2}{Qr} + \left[\frac{4r}{Q^2n}\right],$$

где $\frac{4r}{Q^2n}$ можно интерпретировать как артефакт доказательства, возникающий из-за $\sqrt{n}$ возникающем в неравенстве, связывающем норму вектора с его операторной нормой. Наконец:

$$\beta > \frac{8Sn}{Q^2} + \frac{2n}{Q} - \frac{2n}{Qr} + \left[\frac{4r}{Q^2}\right]. \tag{18}$$

Если взять оригинальный случай $r = 1$, не использовать операторную норму и не опускать единицы, то мы в точности получим заявленный в эвристике результат.

5 Теоретическое сравнение subfield norm, subfield trace и full lattice подходов

Как это было упомянуто ранее, помимо редукции полной решётки (подход full lattice), можно рассмотреть подрешётку $\mathcal{L}'$, соответствующую подполю исходного числового поля. Спуск из исходной решётки в подрешётку можно произвести при помощи отображения нормы (subfield norm) или отображения следа (subfield trace). Данный пункт посвящён сравнению асимптотики минимального значения β, необходимого для успешного нахождения короткого вектора в соответствующей решётке для вышеупомянутых подходов.

Ключевым инструментом детектирования факта нахождения короткого вектора является [DvW21] выполнение неравенства:

$$\mathrm{Vol}(\mathcal{L}^{GF}) < q^{\frac{m-1}{2}} \cdot \alpha_\beta^{\frac{(m-1)^2}{2}}, \tag{19}$$

где m - длина участка BKZ профиля, соответствующего его наклонной части в соответствии с ZGSA.

Благодаря неравенству Адамара мы можем ограничить сверху значение $\mathrm{Vol}(\mathcal{L}^{GF})$ как $||f'||^{\dim/2}$, где $||f'||$ является длиной кратчайшего вектора, а dim - размерность решётки. Это неравенство справедливо, так как объём ограничивается корнем квадратным из произведения dim кратчайших векторов решётки, но они имеют одинаковую длину и по сути являются ротациями $(x^i \cdot f | x^i \cdot g)$ многочленов f и g, рассматриваемых как конкатенацию векторов [DMHS20]. Учтём, что $||g|| \approx ||f|| = B$ и получим вышеупомянутое уравнение.

В случае полной решётки положим $B = ||f||$ тогда:

$$\begin{aligned} B^n &\geqslant q^{\frac{m-1}{2}} \cdot \alpha_\beta^{\frac{(m-1)^2}{2}} \\ \alpha_\beta &\geqslant \left[B^{n/2} \cdot q^{\frac{1-m}{2}} \right]^{\frac{-2}{(m-1)^2}}. \end{aligned}$$

Согласно (8) имеем $\log \alpha_\beta \approx \frac{2 \log \beta}{\beta}$. Также, заметим, что $m - 1 \approx \frac{\ln q}{2 \ln \alpha_\beta}$. Тогда:

$$\begin{aligned} \ln \alpha_\beta &\geqslant \frac{\ln q}{m-1} - \frac{n \ln B}{(m-1)^2} \\ 1 &\geqslant 2 - \frac{n \ln B \cdot 4 \ln \alpha_\beta}{\ln q^2} \\ \ln q^2 &\leqslant n \ln B \cdot 4 \ln \alpha_\beta. \end{aligned}$$

И, наконец, для редукции полной решётки получим:

$$\frac{\beta}{\ln \beta} \leqslant \frac{8n \ln B}{\ln^2 q}. \tag{20}$$

В случае решётки, соответствующей спуску при помощи отображения следа имеем $||f|| \approx rB$. Эта оценка следует из неравенства $||\mathrm{Tr}_{L/K}(f)|| \leqslant [L : K] \cdot ||f||$. Тогда по аналогии с прошлым случаем:

$$\alpha_\beta \geqslant \left[(rB)^{n/2} \cdot q^{\frac{1-m}{2}}\right]^{\frac{-2}{(m-1)^2}}.$$

И, наконец, для спуска при помощи следа:

$$\frac{\beta}{\ln \beta} \leqslant \frac{8n \ln rB}{\ln^2 q}. \tag{21}$$

В случае со спуском при помощи нормы используем следующее неравенство: $||\mathcal{N}_{L/K}(f)|| \leqslant \sqrt{n} \cdot ||f||^{[L:K]}$, где $\mathcal{N}_{L/K}(f)$ - относительная норма элемента $f \in L$ над полем K. В таком случае по аналогии имеем:

$$\alpha_\beta \geqslant \left[\sqrt{n}(B)^{rn/2} \cdot q^{\frac{1-m}{2}}\right]^{\frac{-2}{(m-1)^2}}.$$

И, наконец, для спуска при помощи нормы:

$$\frac{\beta}{\ln \beta} \leqslant \frac{8nr \ln B + \ln n}{\ln^2 q}. \tag{22}$$

Значение $\ln n$ в знаменателе можно опустить ввиду его пренебрежительно малой величины: в асимптотике оно опускается естественным образом. Это неравенство не противоречит (18), так как параметр r в нём заносится под множитель S.

С теоретической точки зрения асимптотическая величины параметров β вызова BKZ алгоритма, располагаются в порядке убывания следующим образом: самым неэффективным показывает себя подход через норму. За ним следует спуск при помощи следа. Наконец, наименьший параметр β даёт подход с редукцией полной решётки.

6 Результаты численных экспериментов

Для проверки теории нами были проведены эксперименты на 20 наборах ключей при выбранных параметрах $n = 64, q = 1777$. Методология эксперимента была по большей части взята из [DvW21]. Для сравнения минимального параметра β, необходимого для обнаружения вектора из плотной подрешётки в полной решётке ($r = 1$), и минимального β необходимого для обнаружения вектора из плотной подрешётки в подрешётки размерности $3n/2$ (случай $r = 2$), на данном ключе (блочной матрице с $rot(h)$ внутри) запускались два процесса редукции: на самой блочной матрице с $rot(h)$ и на ней же, но с $n/2$ вычеркнутыми строками и столбцами, вычеркнутыми согласно пункту 2.1.

Согласно предположению, основанному на выкладках, параметр β при $r = 2$ будет отличаться от оригинального (при $r = 1$) на $\frac{2n(r-1)}{Q}$ и при $r = 2, q = 1777, n = 128$ разница $\beta_{r=2} - \beta_{r=1} \approx 84$. Однако эта оценка асимптотическая, а, значит, обладающая низкой точностью, поэтому в эксперименте мы при нахождении в полной решётки искомого вектора давали подрешётке проработать ещё постоянное для фиксированного n число циклов перебора значения β (в данном случае: 14), после чего эксперимент завершается и запускается следующий.

№ эксперимента	$r = 1$	$r = 2$
0	19	>33
1	19	23
2	16	>30
3	22	19
4	17	>31
5	19	>33
6	17	>31
7	19	>33
8	17	11
9	17	>31
10	17	11
11	17	>31
12	19	>33
13	16	11
14	16	>30
15	17	>31
16	19	>33
17	17	>31
18	18	>32
19	17	>31

Когда в таблице лежат элементы вида $> m$ это означает, что данный эксперимент завершился раньше, чем была найдена соответствующая β.

Данный эксперимент показывает увеличение необходимого для отыскания короткого вектора параметра β при исключении измерений, что говорит в пользу теоретических выкладок, представленных в предыдущем пункте. Тем не менее, набор экспериментальных данных невелик, и для точной оценки корректности теории требуется большее количество вычислительных экспериментов.

Список литературы

[DMHS20] Gabrielle De Micheli, Nadia Heninger, and Barak Shani. Characterizing overstretched ntru attacks. *Journal of Mathematical Cryptology*, 14(1):110–119, 2020.

[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. In *Advances in Cryptology – EUROCRYPT 2017*, pages 3–26, 2017.

[May99] Alexander May. Cryptanalysis of NTRU. *preprint, February*, 1999.