СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Решёточные криптосистемы появились в 1990-е годы как ответ на потребность в алгоритмах шифрования на открытом ключе, устойчивых к атакам с использованием квантовых алгоритмов. Их отличие состоит в том, что проблема редукции базиса решёток, мешающая злоумышленнику вскрыть зашифрованное сообщение, является предположительно устойчивой к атакам, выполняемым на квантовых компьютерах при использовании соответствующих алгоритмов [6].

В частности, неподдельный интерес в среде криптографов вызвала криптосистема NTRU, представленная Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman в районе 1996-го года [7]. Эта криптосистема среди прочих постквантовых обещала более короткие ключи и высокую производительность. Однако проблема однозначного расшифрования сообщения так и не была решена: сообщение с исчезающе малой, но всё же ненулевой, вероятностью могло не зашифроваться на данном ключе [6]. Также, несмотря на улучшенную производительность по сравнению с конкурирующими постквантовыми решениями, NTRU всё же страдала неоптимизованностью. Имменно поэтому в Августе 2017 г. В своей статье [1] Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, и Christine van Vredendaal привели “готовый к практическому применению” вариант NTRU под названием NTRU Prime. Главными достижениями их подхода являются сокращённая длина ключа, оптимизированная производительность и гарантия возможности расшифровки сообщения. Однако, ценой такого выигрыша в случае с системами гомоморфного шифрования является потенциально “растянутый” (англ. Overstretched) параметр q, что может привести к возможной уязвимости к атакам с использованием подрешёток малого ранга, как это описано в [2].

Так как все криптосистемы из семейства NTRU подразумевают структуру так называемой NTRU решётки, то все они будут уязвимы к предлагаемой в данной статье атаке при соблюдении условий для её применимости. На данный момент NTRU-HRSS является кандидатом на стандартизацию NIST[1] и именно поэтому актуальной задачей является уточнение допустимых параметров при проектировании криптосистемы с конкретными параметрами.

Для взлома криптосистемы достаточно провести успешную редукцию решётки $\begin{pmatrix} qI_n & M_h \\ 0_n & I_n \end{pmatrix}$, где M_h - матрица размера $n \times n$ получаемая некоторым образом из открытого ключа, а q достаточно большое простое число.

С момента публикации криптосистемы NTRU был предложен целый перечень атак [2][9][**?**]. Среди них можно выделить три подхода к их построению: комбинаторный [9], решётчатый [1] и гибридный, объеденяющий идеи двух предыдущих.

Целью данной научно-исследовательской работы является исследование асимптотической и конкретной сложностей проведения атак на решётчатые криптосистемы, использующих подрешётки малых рангов. В ходе работы выполнялись следующие задачи:

- анализ зависимости оптимальных параметров BKZ алгоритма от параметров n, q криптосистемы NTRU, где n является количеством коэффициентов открытого ключа, а параметр q представляет собой

[1]Подробную информацию можно найти на сайте `https://csrc.nist.gov/projects/post-quantum-cryptography`

число по модулю которого призводятся вычисления;

- составление программы, возвращающей асимптотическую сложность взлома NTRU Prime как яркого примера представителя семейства криптосистем NTRU на заданных параметрах при подходе, испольщующем редукцию решётки;
- анализ атаки методом подколец.

ГЛАВА 1. ВВОДНЫЕ СВЕДЕНИЯ

1.1 Основные определения и их следствия

Пусть $v_1, \ldots, v_n \in \mathbb{R}^m$ – множество линейно независимых векторов. Множество $\mathcal{L}$ их комбинаций с целочисленными коэффициентами называется решёткой, порождённой этими векторами. Иными словами:

$$\mathcal{L} = \{a_1 v_1 + a_2 v_2 + \ldots + a_n v_n | a_i \in \mathbb{Z}\}.$$

Если все коэффициенты a_i являются целочисленными, то и такая решётка $\mathcal{L}$ тоже называется целочисленной.

Пусть $v_1, \ldots, v_n \in \mathbb{R}^m$ – базис решётки $\mathcal{L}$. Определим векторы $w_i = a_{i_1} v_1 + \ldots + a_{i_n} v_n, 1 \leqslant i \leqslant n$, принадлежащие $\mathcal{L}$. Для решётки над понечным полем коэффициенты $a_{i,j}$, где $1 \leqslant i, j \leqslant n$ целочисленны по определению. Выразим v_i через w_i. В процессе нам понадобится матрица, обратная к матрице:

$$A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}.$$

Однако, вспомним, что коэффициенты A^{-1} тоже должны быть целочисленными, поэтому можно сделать вывод о том, что все базисы решётки $\mathcal{L}$ связаны между собой целочисленными матрицами с определителем, равным ± 1 [6].

Дискретной аддитивной подгруппой в $\mathbb{R}^m$ называется такое множество $\mathcal{L}$, что:

1. $\mathcal{L}$ является подгруппой в $\mathbb{R}^m$;

2. Верно утверждение:

$$\forall v \in \mathcal{L}; \exists \epsilon > 0 : L \cap \{w \in R^m : |v - w| < \epsilon\} = v,$$

где $|\cdot|$ озханает евклидову норму.
Тогда решётка $\mathcal{L}$ является аддитивной подгруппой в R^m.

Фундаментальным параллелепипедом решётки $L = \{a_1 v_1 + a_2 v_2 + + \ldots + a_n v_n | a_i \in \mathbb{R}\}$ называется множество:

$$\mathcal{F}(v_1, \ldots, v_n) = \{t_1 v_1 + \ldots + t_n v_n | t_i \in (0; 1], \forall i \in \{1, \ldots, n\}\}$$

Тогда для любого $w \in \mathbb{R}^n$ верно $w = t + v$, где $t \in (v_1, \ldots, v_n), v \in \mathcal{L}$.

Оказывается [6], что объём фундаментального параллелепипеда является инвариантом решётки, то есть не зависит от выбранного базиса. К тому же он равен определителю решётки:

$$Vol\,\mathcal{F} = \det\,\mathcal{L} = \left| \det \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \right| \leqslant \prod_{i=1}^{n} |v_i|.$$

Рассмотрим некоторые из основных задач из теории решёток, лежащих в основе решётчатых криптосистем:

- **SVP** (shortest vector problem). Проблема поиска кратчайшего вектора. Заключается в отыскании такого вектора $w \in \mathcal{L}(v_1, \ldots, v_n) \setminus \{0\}$, что его норма минимальна.
- **CVP** (closest vector problem). Проблема поиска ближайшего вектора. По данному вектору $w \in \mathbb{R}^n$ найти такой вектор $v \in \mathcal{L}(v_1, \ldots, v_n)$, что норма $|v - w|$ минимальна.

Отметим, что решение вышеизложенных задач не всегда единственно.

В криптоанализе решёточных криптосистем нам важны оценки длины кратчайшего вектора а также “качества” базиса. Чем более ортогональный базис нам дан, тем легче удаётся решить вышеизложенные проблемы. Именно из этих соображений приведём следующие результаты:

Теорема (Эрмита/Минковского). Каждая решётка L размерности n содержит ненулевой вектор v, удовлетворяющий следующему неравенству:

$$|v| < \sqrt{n}(\det \mathcal{L})^{1/n}. \tag{1}$$

Также примечательным является утверждение, что для фиксированной размерности n существует такая постоянная γ_n, называемая Эрмитовой постоянной, что для любой решётки $\mathcal{L}$ размерности n верно:

$$\exists v \in \mathcal{L} \setminus 0 : |v|^2 \leqslant \gamma_n (det\,\mathcal{L})^{2/n}.$$

Ещё один вариант теоремы Эрмита нам понадобится для непосредственного криптоанализа атаки. Он утверждает, что для данной решётки L размерности n существует базис $v_1, \ldots, v_n$, удовлетворяющий следующему неравенству:

$$\prod_{i=1}^{n} |v_i| = det\,\mathcal{L}. \tag{2}$$

Тогда, исходя из данного утверждения, можно определить числовую характеристику $H(B)$ “качественности” базиса $B = (v_1, \ldots, v_n)$, называемую коэффициентом Адамара следующим образом:

$$H(B) = \left(\frac{det\,\mathcal{L}}{\prod_{i=1}^{n} |v_i|} \right)^{1/n}.$$

Тогда она будет лежать в промежутке $(0;1]$, причём будет равна единице тогда и только тогда, когда базис является ортогональным в $\mathbb{R}^m$.

Также, для криптоанализа нам потребуются следующие оценки, касающиеся кратчайших векторов и базисов решётки:

Гауссова эвристика. Для любой решётки $\mathcal{L}$ ранга k имеем:

$$\lambda_1(\mathcal{L}) = \sqrt{\frac{k}{2\pi e}} Vol(\mathcal{L})^{1/k}, \tag{3}$$

где $\lambda_1(\mathcal{L})$ - длина кратчайшего вектора решётки.

BKZ-эвристика. Пусть $b_1, \dots, b_k$ – базис решётки $\mathcal{L}$ ранга k. Тогда при вызове алгоритма BKZ с параметром β, задающим величину блока, применимо к данному базису мы получим:

$$|b_i^*| \leqslant \delta_\beta^2 |b_{i+1}^*|,$$

где $\delta_\beta = (\frac{\beta}{2\pi e}(\pi\beta)^{1/\beta})^{\left(\frac{1}{2(\beta-1)}\right)}$- эрмитов фактор, а $1 \leqslant i \leqslant k-1$.

Применим данную оценку к $\prod_{i=1}^{k} |b_{k+i}^*|$ и получим, что:

$$\delta_\beta^{-k(3k-1)} \cdot |b_1|^k = \prod_{i=1}^{k} |b_{k+i}^*|. \tag{4}$$

Лемма Патаки-Турала. [10] Пусть $\mathcal{L}$ решётка полного ранга, равного n и $b_1, \dots, b_n$ – её базис. Тогда для любой подрешётки $\mathcal{L}' \subset \mathcal{L}$

ранга $d \leqslant n$ имеем:

$$\min_{\substack{S\subset[n];\\|S|=d}} \prod_{|b_i^*|} \leqslant Vol\mathcal{L}' \qquad (5)$$

Теперь рассмотрим $P_n(X) \subset \mathbb{Z}[X]$– множество многочленов степени, не превышающей $n-1$. Пусть также задана решётка $\mathcal{L}(v_0, \ldots, v_{n-1})$ размерности n. Тогда можно ввести гомоморфизм аддитивных групп:

$$\sigma : P_n(X) \to \mathcal{L} : \sigma\left[a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_1X + a_0\right] =$$

$$= a_1v_0 + \ldots + a_nv_n - 1. \qquad (6)$$

Так как множество элементов решётки бесконечно, криптография на практике использует её факторгруппу по заданному отношению эквивалентности. Тогда будем обозначать кольца $\mathbb{Z}[x]/(x^p - x - 1)$ и $\mathbb{Z}/\left(q \cdot \mathbb{Z}\right)[x]/(x^p - x - 1)$, использующиеся в NTRU Prime, заданную параметрами n, q, где q - простое, как R и R/q соответственно.

1.2 NTRU Prime и связь с решётками

Конкретная реализация Streamlined NTRU Prime зависит от трёх параметров (p, q, t), причём для того, чтобы не было проблем с нерасшифровываемыми сообщениями, необходимо выполнить следующие условия: $t \geqslant 1; p \geqslant 3t; q \geqslant 32t + 1$ а многочлен $x^p - x - 1$ неприводим в кольце $(\mathbb{Z}/q)[x]$. В статье [1] предложено выбрать $p = 761; q = 4591; t = 143$. Рассмотрим процесс генерирования пары открытого и секретного ключа:

- Генерируем случайный малый многочлен $g \in R$ пока не получим обратимый в $R/3$ многочлен;

- Генерируем случайный t-малый многочлен (имеющий в ровности t ненулевых коэффициентов)) $f \in R \setminus \{0\}$. Заметим, что, так как он ненулевой, то он обратим в R/q ввиду того, что $t \geqslant 1$;
- Вычислим $h = g/(3f)$, выполняя операции в кольце R/q и получим открытый ключ;
- Сохраним секретные ключи: $f \in R, g = g \pmod 3 \in R/3$.

Streamlined NTRU Prime является по сути механизмом инкапсуляции ключа (key encapsulation mechanism), что означает, что шифрующая сторона (Алиса) получает на вход открытый ключ, а возвращает шифротекст с сессионным ключом. Однако асимметричная криптография редко используется для передачи непосредственно сообщений ввиду долгого процесса зашифровки и расшифровки, поэтому договоримся считать, что исходным сообщением является случайный элемент из множества исходных сообщений. Рассмотрим процесс зашифрования сообщения, представленного в виде многочлена r (инкапсуляция):

- Генерируем случайный t-малый элемент $t \in R$;
- Находим $hr \in R/q$;
- Округляем каждый коэффициент многочлена hr, рассматриваемый как число в промежутке $[-(q-1)/2, (q-1)/2]$ до ближайшего кратного числу 3, получая $c \in R$.
- Вычисляем хеш значение для r. Подойдёт любая хеш функция, пригодная для криптографического применения. Например, SHA-256.;
- Результатом работы алгоритма является пара (C, c).

Далее рассмотрим процесс расшифрования:

- Умножим c на $3f$ над R/q;
- Рассмотрим каждый коэффициент многочлена $3fc$ как число в

промежутке $[-(q-1)/2, (q-1)/2]$ и приведём по модулю 3, получив многочлен $e \in R/3$;

- Домножим e на $1/g$ над кольцом $R/3$;
- Переведём e/g в кольцо R так, чтобы он оказался малым (его коэффициенты по модулю не должны превышать 1) и получим многочлен r';
- Зная r', вычислим C' и c', домножив его на h;
- Если r' t-мал и $(C, c) = (C', c')$ то подаём на выход r', иначе возвращаем сообщение об ошибке декодирования.

Если (C, c) принадлежит множеству исходных сообщений, то он получен округлением коэффициентов многочлена hr до ближайшего числа, кратного 3. Например $c = m + hr \in R/q$, где m мал. Все коэффициенты многочлена $3fm + gr \in R$ в промежутке $[-16t, 16t]$ и попадают в промежуток $[-(q-1)/2, (q-1)/2]$, так как $q \geqslant 32t + 1$. Если рассмотреть каждый коэффициент $3f = 3fm + gr$ как число в промежутке $[-(q-1)/2, (q-1)/2]$, то мы перейдем в кольцо R и после приведения по модулю 3 получим $gr \in R$. Тогда $(gr)/g = r \in R/3$. Переход обратно к R не изменяет r, как как он мал. Тем самым доказывается корректность алгоритма шифрования.

Как это было упомянуто в 1.1, благодаря гомоморфизму (6) мы имеем вложение кольца многочленов R в решётку $\mathcal{L}$.

Когда мы работаем с криптосистемой NTRU, нами используется особый тип решётки - $(L)_h$ так называемой “NTRU решёткой” [8] размерности $2n$, порождаемой векторами, компоненты которых являются строки следующего вида:

$$\mathcal{L}_h = \left\{(f, g) \in R^2 \colon q \equiv hf/p \pmod q\right\}.$$

Причём, дискриминант решётки: $\det \mathcal{L}_h = q^n$.

Несмотря на то, что алгоритм шифрования NTRU Prime отличается от классического NTRU, решётка, появляющаяся при анализе, имеет тот же вид. Она имеет подрешётку ранга n, базис которой составлен из строк вида $x^i(f, g), 0 \leqslant i \leqslant n-1$.

ГЛАВА 2. АТАКИ С ИСПОЛЬЗОВАНИЕМ ПОДРЕШЁТОК МАЛОГО РАНГА

2.1 Атака методом редукции решётки. Её асимптотическая сложность

Предположим, дана постановка задачи: пусть $h = f/g \pmod q \in \mathbb{Z}_q[x]/\Phi$, где Φ – неприводимый полином с целыми коэффициентами. Требуется найти f, g с малыми коэффициентами зная h, n, m, q.

Приведём алгоритм взлома из статьи [2] с оригинальными обозначениями:

1. Выбираем размер блока $\beta = \Theta\left(\frac{n \log q}{\log^2 q} \log\left(\frac{n \log q}{\log^2 q}\right)\right)$, использующийся в BKZ алгоритме, подсчитываем согласно эвристике Гаусса $\delta_\beta \approx (\beta/(2\pi e) \cdot (\pi\beta)^{1/\beta})^{1/(2(\beta-1))}$ ищем наименьшее k не удовлетворяющее условию:

$$\left(\frac{k}{2\pi e}\right)^{k/2} \cdot q^k \geqslant \delta_\beta^{k(3k-1)} (n/2)^n.$$

2. Комбинируем алгоритм Коркина-Золотарёва и эффективный детерминированный SVP алгоритм [3] применяемый для получения первого вектора. Применяем этот алгоритм для редукции решётки, порождаемой базисом $\begin{pmatrix} q\, I_n & M_h^{\mathcal{O}} \\ 0 & I_n \end{pmatrix}$ где $M_h^{\mathcal{O}}$ определяется как матрица линейного отображения:

$$M_{\mathrm{a}}^{\mathcal{L}} : \mathcal{L} \to 0;\ x \to \mathrm{a} \cdot x.$$

   В итоге получаем редуцированный базис $b_i^* : 1 \leqslant i \leqslant n/2$.

3. При помощи редуцированного базиса, векторы которого лежат в $\begin{pmatrix} \mathrm{f} \\ \mathrm{g} \end{pmatrix} \cdot \mathcal{O}$ находим f, g, где $\mathcal{O}$ порядок числового поля K [2].

Проанализируем сложность данного подхода, учитывая свойство NTRU решёток, заключающееся в том, что в ней есть n коротких векторов.

Приведём матрицу базиса к следующему виду:

$$\begin{pmatrix} q \cdot I_{n-k} & 0 & 0 & 0 \\ 0 & q \cdot I_k & 0 & 0 \\ C_{00} & C_{01} & I_k & 0 \\ C_{10} & C_{11} & 0 & I_{n-k} \end{pmatrix},$$

где $0 < k \leqslant n$.

Обозначим теперь:

$$B' = \begin{pmatrix} q \cdot I_k & 0_k \\ C_{01} & I_k \end{pmatrix}.$$

Применим к B' алгоритм BKZ с размером блока β. Согласно [2] сложность его применения оценивается как $2^{O(\beta)}$. Выбрав

$$\beta = \Theta\left(\frac{n\log(\sigma)}{\log^2 q} \log\left(\frac{n\log(\sigma)}{\log^2 q}\right)\right),$$

где σ – параметр распределения коэффициентов в многочлене f, заметим, что определение растянутого (overstretched) параметра q подразу-

[2] Подробнее это обсуждается в пункте 2.3 данной работы.

мевает следующее: $q = 2^{\alpha\sqrt{n}}$. Тогда:

$$\beta = \Theta\left(\frac{n\log(\sigma)}{\log^2 2^{\alpha\sqrt{n}}}\log\left(\frac{n\log(\sigma)}{\log^2 2^{\alpha\sqrt{n}}}\right)\right) = \Theta\left(\frac{\log(\sigma)}{\alpha^2\log^2 2}\log\left(\frac{\log(\sigma)}{\alpha^2\log^2 2}\right)\right).$$

Подставим этот результат в оценку сложности BKZ и заменим Θ на O:

$$2^{O(\beta)} = 2^{O\left(\frac{\log(\sigma)}{\alpha^2\log^2(2)}\log\left(\frac{\log(\sigma)}{\alpha^2\log^2(2)}\right)\right)} = O\left(\left(2^{\log\left(\frac{\log(\sigma)}{\alpha^2\log^2(2)}\right)}\right)^{\frac{\log(\sigma)}{\alpha^2\log^2(2)}}\right) =$$

$$= O\left(\left(\frac{\log(\sigma)}{\alpha^2\log^2(2)}\right)^{\frac{\log(\sigma)}{\alpha^2\log^2(2)}}\right) =$$

$$= O\left(\left(\frac{1}{\alpha^2\log^2 2}\right)^{\frac{\log(\sigma)}{\alpha^2\log^2 2}} \cdot \left(\sigma^{\log\log(\sigma)}\right)^{\frac{1}{\alpha^2\log^2 2}}\right) =$$

$$= O\left(\sigma^{-\log\left(\alpha^2\log^2\sigma\right)/\left(\alpha^2\log^2\sigma\right)+\log\log(\sigma)/(\alpha^2\log^2\sigma)}\right) =$$

$$= O\left(\sigma^{[\log\log(\sigma)-\log(\alpha^2\log 2)]/(\alpha^2\log 2))}\right)$$

где σ -параметр для распределения, согласно которому был сгенерирован достаточно малый многочлен f. Как мы можем видеть, сложеость BKZ алгоритма теперь не зависит непосредственно от n, однако зависимость от σ и α остаётся. Согласно [2] σ это среднеквадратичное отклонение нормы вектора, выбранного NTRU распределением, от его математического ожидания. Математическое ожидание евклидовой нормы вектора v, выбранного равномерным на множестве $\{-1, 0, 1\}^n$

распределением D_n есть:

$$\mathbb{E}(|D_n|) = \sqrt{2n/3}$$

Для того, чтобы оценить параметр σ, являющийся корнем квадратным от дисперсии распределения D_n, нам необходимо для начала найти эту дисперсию:

$$\mathbb{D}(D_n) = \mathbb{E}\left(\mathbb{E}(|D_n|) - |D_n|\right)^2 \tag{7}$$

Так как распределение D_n состоит из равновероятностного и независимого выбора одного из трёх элементов n раз, то оно само является равномерным на множестве наборов $i \in \{-1, 0, 1\}^n$. Распишем определение математического ожидания применительно к (7):

$$\mathbb{D}(D_n) = 3^{-n} \sum_{i \in -1,1,0} \left(\sqrt{2n/3} - \sqrt{\sum_{j=0}^{n-1} i_j^2} \right)^2 =$$

$$= 3^{-n} \sum_{i \in -1,1,0} \left(\sqrt{2n/3} - \sqrt{\sum_{j=0}^{n-1} |i_j|} \right)^2 =$$

$$= 2n/3 + 3^{-n} \sum_{i \in \{-1,1,0\}^n} \left(\sum_{j=0}^{n-1} |i_j| - \sqrt{\frac{8n}{3} \sum_{j=0}^{n-1} |i_j|} \right) =$$

$$= 2n/3 + 3^{-n} \sum_{i \in \{-1,1,0\}^n} \left(\mathrm{wt}(i) - \sqrt{\frac{8n}{3} \mathrm{wt}(i)} \right).$$

Для набора $i \in \{-1, 0, 1\}^n$ веса $\mathrm{wt}(i) = w$ существует $\binom{n}{w}$ вариантов выбора мест расположения ненулевых координат. Тогда:

$$\sum_{j=0}^{n-1} \text{wt}(i) = \sum_{w=0}^{n} \binom{n}{w} w$$

И поэтому:

$$\mathbb{D}(D_n) = 2n/3 + 3^{-n} \left[\sum_{i \in \{-1,1,0\}^n} \text{wt}(i) - \sum_{i \in \{-1,1,0\}^n} \sqrt{\frac{8n}{3} \text{wt}(i)} \right]$$

$$= 2n/3 + 3^{-n} \left[\sum_{w=0}^{n} \binom{n}{w} w - \sum_{w=0}^{n} \binom{n}{w} \sqrt{\frac{8n}{3} \cdot w} \right] = 2n/3 + 3^{-n} \left(2^{n-1} n - 3 \cdot 2^{n-4} n^2 \right).$$

Тогда $\sigma = \sqrt{2n/3 + 3^{-n} \left(2^{n-1} n - 3 \cdot 2^{n-4} n^2 \right)} = O(\sqrt{n})$, поэтому его сложность оценивается как:

$$2^{O(\beta)} = O\left((\alpha\sqrt{n})^{\log\log(\sqrt{n}) - \log(\alpha^2 \log 2)/(\alpha^2 \log 2)} \right), \tag{8}$$

где $\alpha > 1$.

Так как $\log\log\alpha\sqrt{n}$,расположенным в степени, можно пренебречь на относительно малых n, использующихся в криптографии, получаем примерно полиномиальную сложность алгоритма в случае с растянутым параметром q. В соответствии с опытом и традициями криптоанализа [11] на решётках предположим, что базис, возвращаемый алгоритмом BKZ удовлетворяет BKZ эвристике В частности это означает, что k последних векторов, возвращаемых алгоритмом малы. По лемме Патаки-Турала (5) их произведение ограничено объёмом любой подрешётке $\mathcal{L}'$ ранга k решётки L. Применим также следствие из

BKZ-эвристики и получим:

$$\delta_\beta^{-k(3k-1)}|b_1'|^k \leqslant \mathrm{Vol}\,\mathcal{L}.$$

Далее можно ввести матрицу X' как это сделано в [11] такую, что $\mathrm{Vol}\,\mathcal{L}' \leqslant \mathrm{Vol}\,\mathcal{L}$ и использовать это значение, как ограничивающее $|b_1'|$. Тогда $|b_1'| \leqslant \delta_\beta^{3k-1}\mathrm{Vol}^{1/k}\mathcal{L}$. С другой стороны пусть $\mathcal{L}^\perp$ - ортогональная проекция $\mathcal{L}(B')$ в векторное пространство, ортогональное к порождаемому X'. Тогда Гауссова эвристика даёт нам:

$$\lambda_1(\mathcal{L}^\perp)^k = \left(\frac{k}{2\pi e}\right)^{k/2} q^k/\mathrm{Vol}(X')$$

Если $|b_1'| < \lambda_1(\mathcal{L}^\perp)$, то $b_1 \in \mathcal{L}(X')$. Чтобы понять, когда это происходит, предположим от противного, что $|b_1'| \geqslant \lambda_1(\mathcal{L}^\perp)$. Тогда:

$$\delta_\beta^{-k(3k-1)}|b_1'|^k \leqslant \mathrm{Vol}\,\mathcal{L}(X');$$

$$\left(\frac{k}{2\pi e}\right)^{k/2} \frac{q^k}{\mathrm{Vol}\,\mathcal{L}(X')} \leqslant |b_1'|^k$$

Тогда перемножим эти два неравенства:

$$\delta_\beta^{-k(3k-1)}\left(\frac{k}{2\pi e}\right)^{k/2} q^k \leqslant \mathrm{Vol}^2\mathcal{L}(X')$$

Для того, чтобы найти параметры k, β заменим $\mathrm{Vol}\mathcal{L}(X')$ на оценку $(n/2)^{n/2}$ и перепишем это в виде:

$$\delta_\beta^{-k(3k-1)}\left(\frac{k}{2\pi e}\right)^{k/2} q^k \geqslant \delta_\beta^{k(3k-1)}(n/2)^{n/2}.$$

Что эквивалентно:

$$\sqrt[k(3k-1)]{\delta_\beta^{-k(3k-1)} \left(\frac{k}{2\pi e}\right)^{k/2}} q^k (n/2)^{-n/2} \geqslant \delta_\beta \tag{9}$$

Данного неравенства достаточно, чтобы относительно быстро подобрать подходящий параметр k, опираясь на значение β, однако точных указаний как выбирать последнее не было дано. Изучим этот вопрос.

В статье [1] приведён критерий выбора β:

$$\log q = \alpha\sqrt{n} \leqslant \sqrt{12n\log(n/2)\log(\delta_\beta)}.$$

Это означает, что для не выполнения неравенства достаточно:

$$\alpha^2/(12\log(n/2)) > \log\delta_\beta.$$

BKZ алгоритм является самым сложным этапом всего алгоритма взлома, поэтому, узнав его асимптотическую сложность, мы получим асимптотическую сложность всей атаки. Она равна $O(2^\beta)$.

2.2 Алгоритм подбора параметров атаки методом редукции решётки

Для нахождения оптимального решения неравенства (8) сначала необходимо изучить его свойства. Для начала отметим, что при росте β минимальный k такой, что неравенство (8) верно, уменьшается. Однако, нас интересует именно минимальный β, так как сложность выполнения атаки асимптотически зависит именно от него. Ссылаясь на [11] отметим, что существует такой β_0, что все $\beta < \beta_0$ не удовлетворяют неравенству (8), а все $\beta \geqslant \beta_0$ удовлетворяют. Поэтому найдём β, применив бинарный поиск. То же самое можно сказать и про k в том же неравенстве, но с зафиксированном β. Параметр k тоже найдём при помощи бинарного поиска. Код алгоритма можно найти в git-репозитории [5].

На рисунках снизу приведены данные, полученные при помощи алгоритма, для случая $n = 128$.

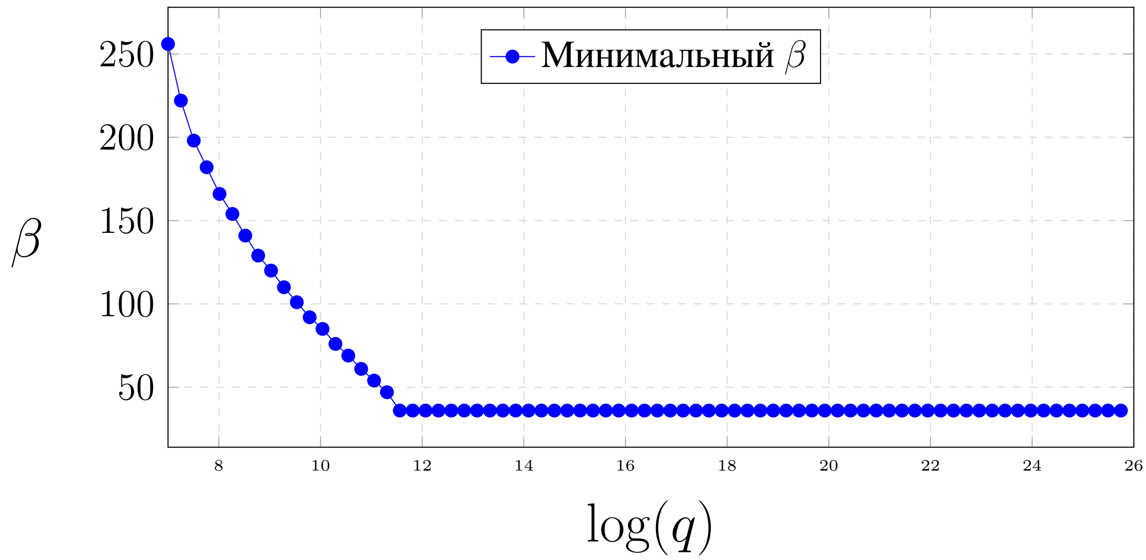

Рис. 1: График зависимости β от $\log(q)$ при $n = 128$

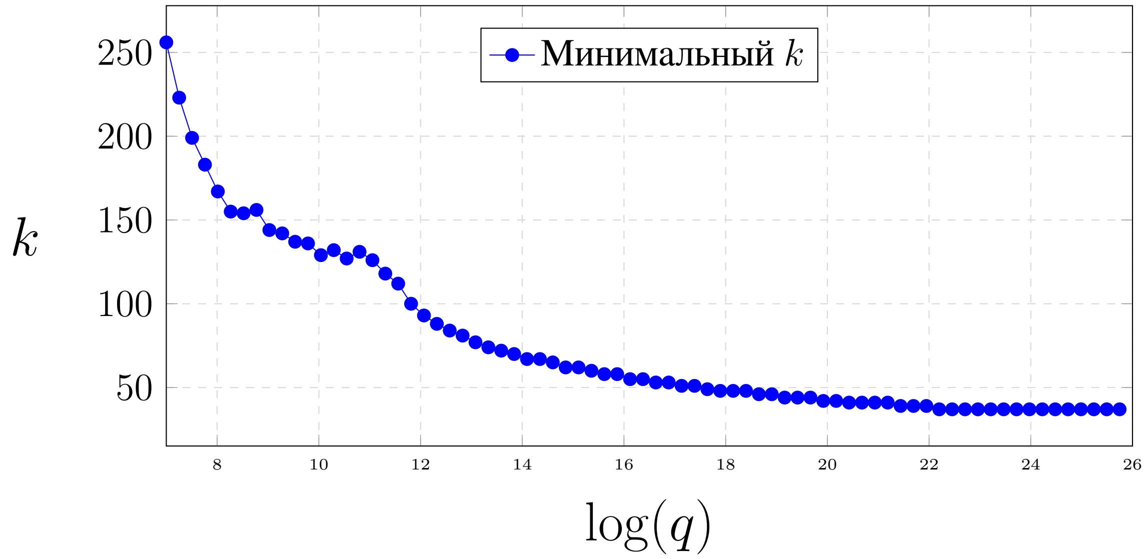

Рис. 2: График зависимости k от $log(q)$ при $n = 128$

На графике видна монотонно убывающая зависимость параметра β от q, продолжающаяся до $q \approx \sqrt{n}$, после чего параметр β выходит на плато. Отметим, что аппроксимация эрмитова фактора $\delta_\beta = (\frac{\beta}{2\pi e}(\pi\beta)^{1/\beta})^{\left(\frac{1}{2(\beta-1)}\right)}$ подходит для относительно больших $\beta \geqslant 50$. Если мы хотим проверить меньшие β, то эрмитов фактор стоит находить при помощи таблиц, составленных эксперементальным путём, или проводя численные эксперименты, то есть запуская на данных параметрах q, n, β BKZ алгоритм и находя δ_β согласно BKZ-эвристике. Плато возникает из-за того, что оценка на δ_β, даваемая BKZ эвристикой, имеет локальный максимум при $\beta \approx 36$ в результате чего разработанный алгоритм не может подобрать $\beta < 36$, если практика его позволяет. Если мы бы испольщовали эксперементальные данные о величине δ_β, то это явление бы исчезло и мы предположительно увидили бы другое продолжение данной кривой. Этим и может быть объяснена эффективность атаки, отличающаяся в лучшую сторону от предсказанной теорией.

Для данного случая $n = 128, 12 \leqslant \log q \leqslant 32$ мною была проведена серия атак, подтверждающая теорию. Её результаты приведены в таблице:

Таблица 1 - Зависимость минимального параметра β, приводящего на практике к успешной атаке, от $log(q)$ при $n = 128$.

$\log q$	12	14	16	18	20	22	24	26	28	30	32
β	39	32	31	31	31	31	31	31	31	31	31
k	128	125	127	127	127	127	127	127	127	127	125

Как можно видеть из содержимого таблицы, атака на практике работает несколько лучше, чем это предсказывает теория. По мере уменьшения $\log q$ и его приближения к $\sqrt{n} \approx 12$ мы видим резкий скачок в значении β, что приводит к более долгой атаке.

Отдельно отметим поведение минимального k такого, что при минимальном β, найденым при помощи алгоритма, неравенство (9) выполняется. Найденный параметр k тоже показывает тенденцию к уменьшению, однако не показывает монотонной зависимости. Это связано с тем, что, как только условия позволяют уменьшить знаение β, параметр k возрастает.

Графики для случаев $n = 256, n = 512, n = 1024$ повторяют свойства:

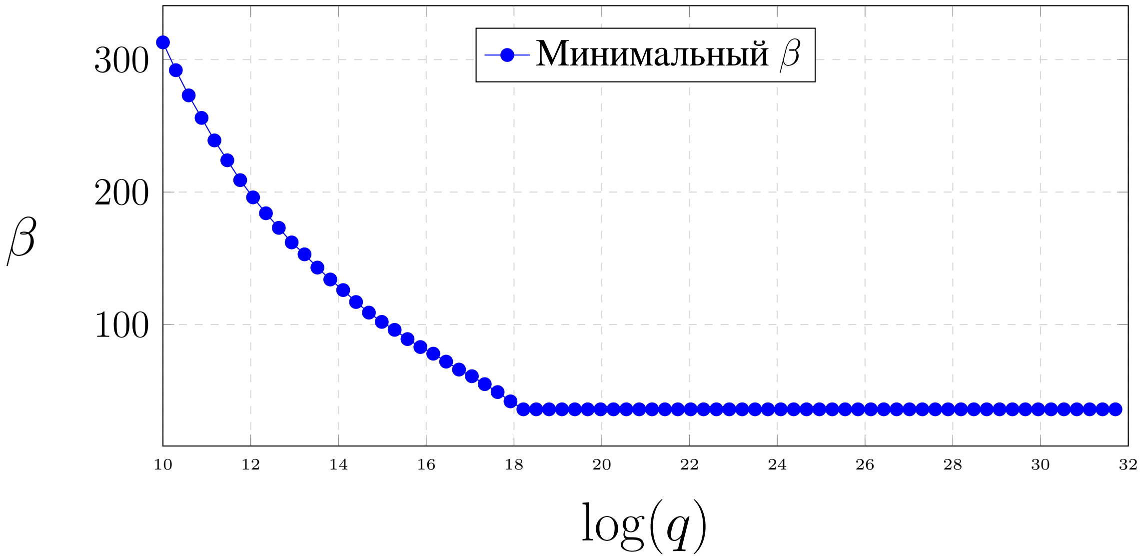

Рис. 3: График зависимости β от $\log(q)$ при $n = 256$

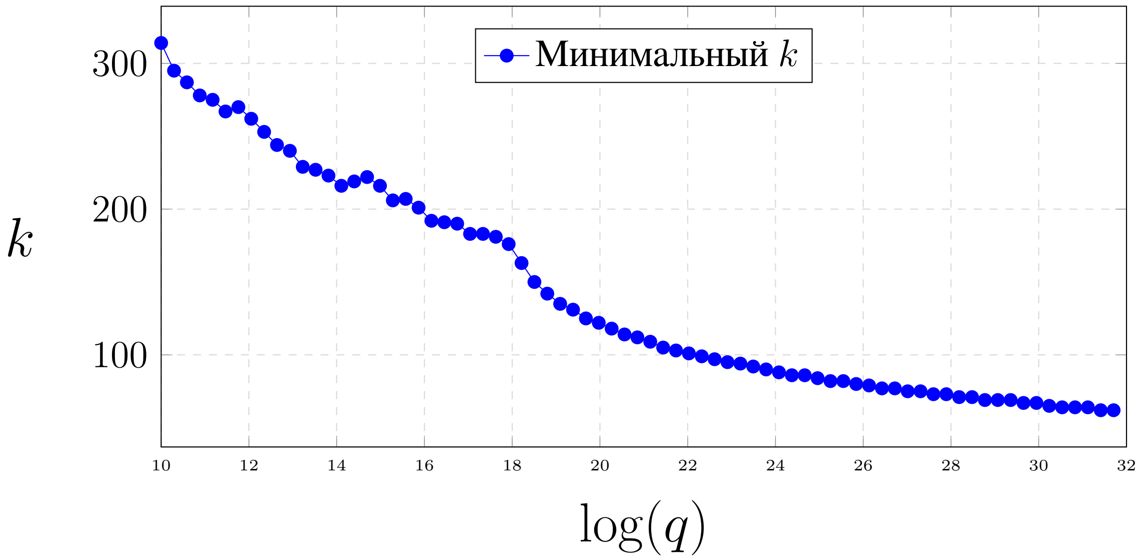

Рис. 4: График зависимости k от $log(q)$ при $n = 256$

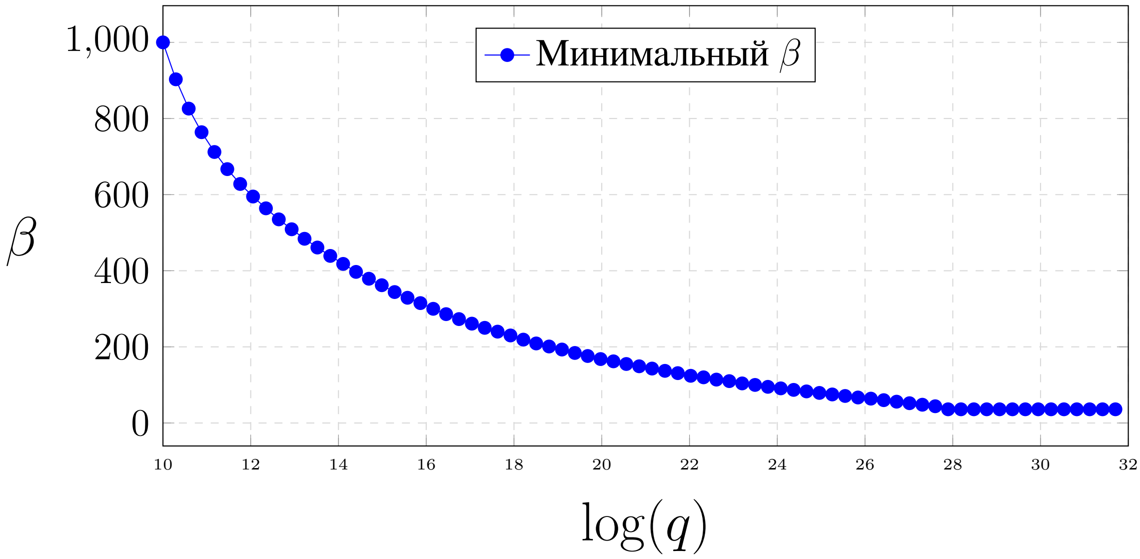

Рис. 5: График зависимости β от $\log(q)$ при $n = 512$

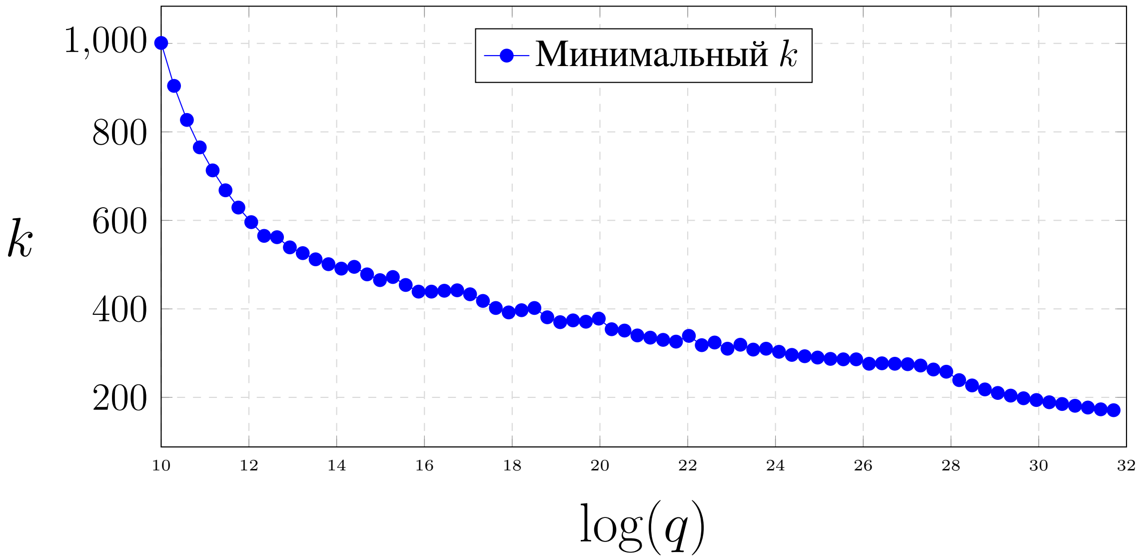

Рис. 6: График зависимости k от $log(q)$ при $n = 512$

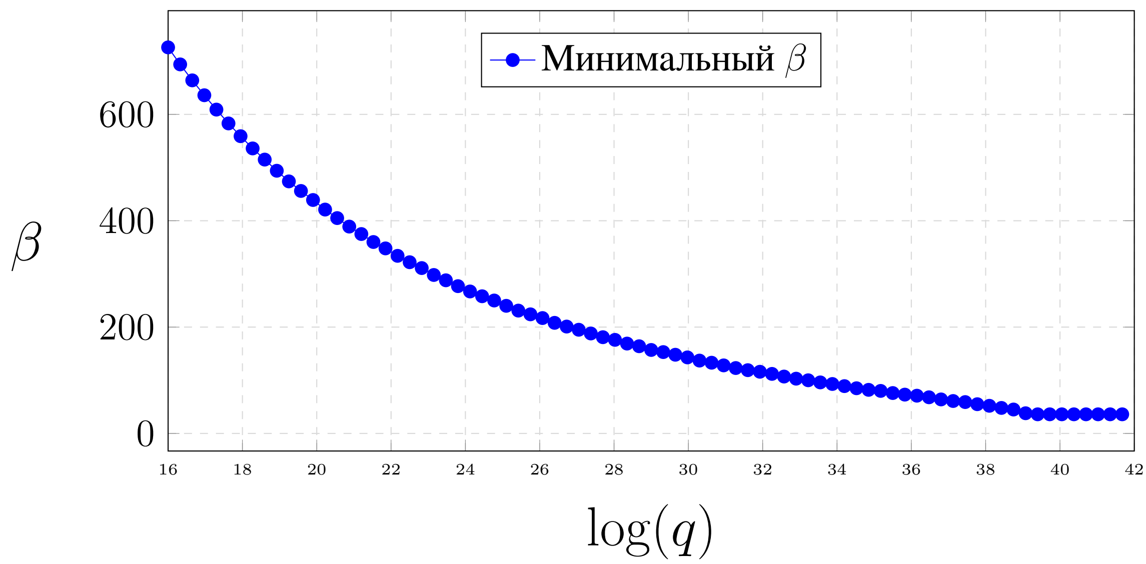

Рис. 7: График зависимости β от $\log(q)$ при $n = 1024$

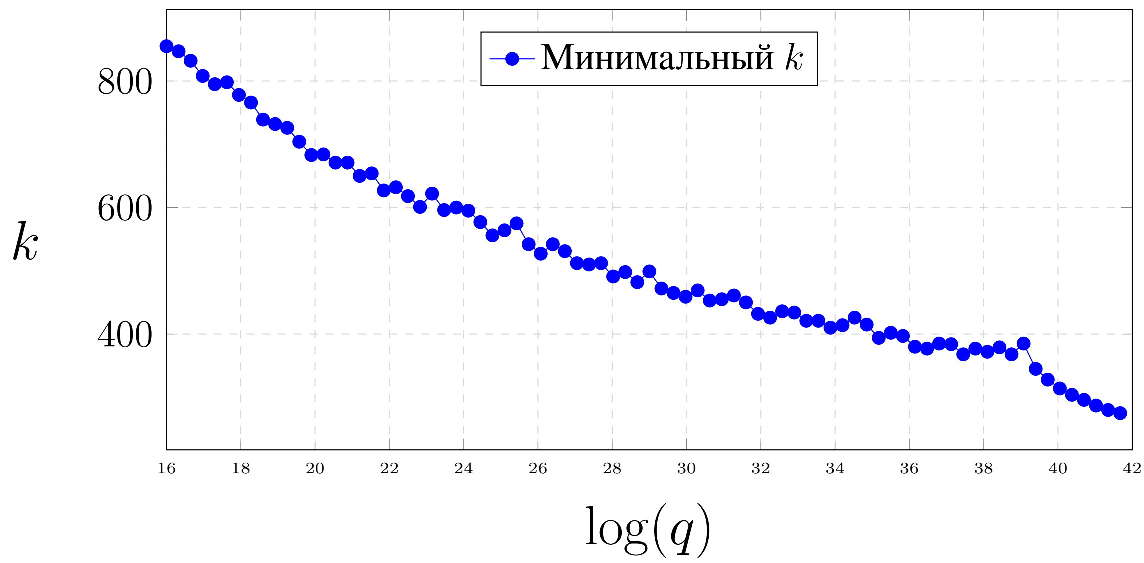

Рис. 8: График зависимости k от $log(q)$ при $n = 1024$

Данный алгоритм был реализован в системе компьютерной алгебры Sage 9.1 [5]. Он опирается на библиотеку fpylll [4], реализующую редукцию базиса решётки.

Интересным вопросом является уточнение данных графиков для малых $\beta \leqslant 50$, найденных экспериментальным путём.

2.3 Обзор атаки с использованием подколец.

В статье [1] предлагается алгебраическая атака на криптосистемы, использующие подрешётки малого ранга. Алгебраической её назвали из-за того факта, что в ней используется умножение на открытый ключ h, который является элементом кольца усечённых многочленов $R_q = (\mathbb{Z}/q\mathbb{Z})[x]/(x^n + 1)$. Для объяснения принципа работы атаки сначала необходимо показать связь между малыми векторами решётки и их нормами, а также отметить, что короткий вектор это вектор $(f\overline{g}, g\overline{g})$, где g является набором коэффициентов многочлена $g(x)$, а $\overline{g}$ - набором коэффицинтов многочлена $\overline{g(x)} = g(1/x)$.

Покажем, что векторы, которые мы ищем являются короткими. Для этого для начала мы покажем, что порядок $\mathcal{O}$ числового поля K, выбираемого на усмотрение проектировщика криптосистемы, стабилен относительно умножения на H. Это может быть проверено подсчётом эрмитовой нормальной формы конкатенации базиса $\sigma(\mathcal{O})$ для всех $\sigma \in H = \{(x_1, \ldots, x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} : x_{s_1+s_2+j} = \overline{x_{s1+j}}, \forall j \in [s_2]\}$, где s_1 и s_2 является числом вещественных и комплексных вложений числового поля K соответственно. После этого мы можем назвать $\mathcal{O}$ порождённым этой матрицей.

Атака состоит в нахождении коротких векторов решётки, порождённой:

$$A = \begin{pmatrix} q \cdot I_n & M_h^{\mathcal{O}_L} \\ 0 & I_m \end{pmatrix}$$

при помощи редукции решетки. Отметим, что h является публичным ключом, так что такой базис может быть построен. Мы хотим показать, что коротким вектором решётки является:

$$\begin{pmatrix} f \cdot N_{K/L}(g)/g \\ N_{K/L}(g) \end{pmatrix},$$

где L - подполе в K, $N_{K/L}$ - алгебраическая норма, определяемая как $N_{K/L}(g) = (-1)^d a_0$, где d это степень миникального многочлена элемента g, а a_0 - его свободный коэффициент.

Пусть $\mathcal{O}_L = \mathcal{O} \cap L$. Тогда верна следующая теорема:

Теорема 1. Существует такой элемент $v \in g\mathcal{O} \cap \mathcal{O}_L$, что с вероятностью $1 - 2^{-\Omega(n)}$ верно:

$$0 < |v| < \sqrt{m}\Delta^{1/(2n)}\sigma^{n/m},$$

где n и m - размерности K и L соответственно над полем рациональных дробей.

Из данной теоремы следует, что для большинства параметров норма кратчайшего ненулевого вектора оценивается как $O(\sigma)^{n/m}$.

В криптографии в качестве поля K используется поле $\mathbb{Q}[X]/(X^n + 1) \cong \mathbb{Q}[\zeta_{2n}]$ и $\mathcal{O} = \mathbb{Z}[X]/(X^n + 1) \cong \mathbb{Z}[\zeta_{2n}]$. Для любого r, делящего n, мы выбираем $L = \mathbb{Q}[X^r]$, поэтому $\mathcal{O}_L = \mathbb{Z}[X^r]$ и $|H| = r$. Поэтому $m = n/r$ является размерностью решётки. Так как $\{X^i, 0 < i \leqslant m)\}$ представляет собой ортогональный базис, координаты f и g являются независимыми случайными дискретными гауссовыми величинами, распределёнными с параметром $s/\sqrt{n}$. Также мы можем непосредственно редуцировать решётку, порождённую A при помощи канонической квадратичной формы при помощи BKZ алгоритма.

Тот факт, что $\mathcal{O}$ является циклотомическим полем степени 2, даёт нам легко определяемый ортогональный базис, позволяющий нам в получить результат в аналитическом виде. В других случаях можно свести задачу к выше рассмотренной при помощи полиномиального алгоритма [11].

Теорема 2. Пусть f, g распределены согласно дискретному гауссову распределению $D_{\mathcal{O},\sigma}$ и $h = f/g \mod q$, являющийся корректно определённым с вероятностью $1 - \varepsilon$, где $0 < \varepsilon < 1$. Пусть также $\sigma = n^{\Omega(1)}$ и $\sigma < q^{1/4}$. Тогда мы можем восстановить ненулевой вектор, кратный (f, g) нормы не превышающей $\sqrt{q}$ за время, оцениваемое как:

$$\exp\left(O\left(\max\left(\log n, \frac{n \log \sigma}{\log^2 q} \log\left(\frac{n \log \sigma}{\log^2 q}\right)\right)\right)\right)$$

с вероятностью неудачи не превышающей $\varepsilon + 2^{-n}$. Причём, в случае, когда:

$$\log q = O\left(\frac{\log^2 q \log n}{n \log\log n}\right),$$

мы получаем полиномиальную атаку.

Сложность данного подхода ко взлому NTRU асимптотически совпадает со сложностью взлома методом решётчатой редукции [1].

ЗАКЛЮЧЕНИЕ

В результате написания данной работы был составлен алгоритм нахождения оптимизированных параметров атаки методом решётчатой редукции, а также был проведён ряд успешных атак на задачу, лежащую в основе криптосистемы NTRU с параметрами $n = 128$ и модулями $q \geqslant 2^{12}$. Полученные в результате исследования сведения могут быть использованы в вычислении и уточнении криптостойкости данной криптосистемы. По результатам эксперемента можно уверенно сказать об эффектитвности подхода и уязвимом значении $\alpha \approx 1{,}061$ для $n = 128$, где $q = 2^{\alpha\sqrt{n}}$.

Интересным вопросом для дальнейшего изучения является нахождение эрмитова фактора для малых $\beta \leqslant 50$ и предсказание поведения BKZ алгоритма именно в этих случаях. Отдельным полем для экспериментов является оценка и проверка времени работы атаки для больших размерностях $n > 128$. Активно разрабатываемая на данный момент библиотека G6K, предоставляющая гибкий инструментарий для распараллеливания вычислений, а также оптимизирующая алгоритм просеивания, часто применяющийся для редукции решётки при больших размерах блока $\beta > 50$ должна на практике ускорить вычисления и позволить расширить диапазон параметров, пригодных для реальных экспериментов.

СПИСОК ИСПОЛЬЗОАННЫХ ИСТОЧНИКОВ

Список литературы

[1] *Changmin Lee, Alexandre Wallet* Lattice analysis on MiNTRU problem - ASIACRYPT 2019 // - 10 с. [электронный ресурс] – URL: https://www.sem anticscholar.org/paper/Lattice-analysis-on-MiNTRU-problem-Lee-Wallet/d 922d602c196bebb2057b734fd8012b1bbb3cb9a (дата обращения 02.12.2020);

[2] *Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, Christine van Vredendaal* NTRU Prime: reducing attack surface at low cost // - 55 с. [электронный ресурс]. – URL: https://eprint.iacr.org/2016/461.pdf (дата обращения 02.12.2020)

[3] *Daniele Micciancio and Panagiotis Voulgaris* Faster exponential time algorithms for the shortest vector problem // - 21st Annual ACMSIAM Symposium on Discrete Algorithms - Austin, TX, USA: ACM-SIAM, 2010 - с. 1468–1480

[4] fplll/g6k [электронный ресурс]. URL: https://github.com/fplll/g6k

[5] git-репозиторий Diploma-NTRU-attack-params-BKZ [электронный ресурс]. URL: https://github.com/alexgit256/Diploma-NTRU-attack-params-BKZ-/blob/main/Optimal%20BKZ%20params%20finder.py

[6] *Hoffstein J., Pipher J., Silverman J.H.* An Introduction to Mathematical Cryptography. – Springer, 2014. - 543 c.;

[7] *Hoffstein J., Pipher J., Silverman J. H.* NTRU: A ring-based public key cryptosystem //International Algorithmic Number Theory Symposium. – Springer, Berlin, Heidelberg, 1998. – С. 267-288.

[8] *Mariano Monteverde.* NTRU software implementation for constrained devices - Leuven: KATHOLIEKE UNIVERSITEIT LEUVEN, 2007 - 70 с. [электронный ресурс]. URL: https://upcommons.upc.edu/bitstream/handle/2099.1/8522/memoria.pdf (дата обращения 02.12.2020);

[9] *Nick Howgrave-Graham, Joseph H. Silverman, William Whyte.* A Meet-In-The-Middle Attack on an NTRU Private Key - Burlington: NTRU Cryptosystems;

[10] *Pataki G., Tural M.* On sublattice determinants in reduced bases //arXiv preprint arXiv:0804.4014. – 2008.

[11] *Phong-Quang NGUYEN,Antoine JOUX, Nigel SMART и проч.* Reduction de reseau et securite concrete du chiffrement completement homomorphe - Париж: UNIVESITE PARIS DIDEROT, 2013 - 144 с.;