УДК 512.5

А. С. Каренин

НАХОЖДЕНИЕ ОПТИМАЛЬНЫХ BKZ-ПАРАМЕТРОВ ДЛЯ РЕДУКЦИИ NTRU-РЕШЕТОК

Рассмотрен вопрос подбора оптимальных параметров для атаки методом редукции решетки с применением BKZ-алгоритма на решетчатые криптосистемы, использующие решетки с подрешетками малого ранга. Иллюстрируются проблемы некоторых подходов к организации таких решетчатых криптосистем. Описаны условия для существования полиномиальной атаки, представлен эффективный алгоритм, находящий параметры для данной атаки. Разработанный алгоритм является довольно быстрым и работает за время, оцениваемое как $O(\log^2 n)$*, где* n *– размерность решетки. Его корректность проверена численными эксперементами. Также приведены графики, связывающие параметры решетки и минимальные необходимые для ее успешной редукции параметры.*

This article is devoted to selection of optimal parameters for lattice reduction attack against lattice-based cryptosystems that use lattices with low rank sublattices. It illustrates design flaws caused by current approach to buiding these types of cryptosystems. Its relevance and novelty lies in the description of the conditions for the existence of a polynomial attack and in constructing an efficient algorithm that allows us to find optimal reduction attack parameters. The algorithm developed during the work on this article is quite fast and requires $O(\log^2 n)$ *of time to return results where* n *is the dimension of lattice. Its correctness has been verified by numerical experiments. As a result, graphs are shown connecting the parameters of the lattice and the minimum smallest parameters necessary for its successful reduction.*

Ключевые слова: криптография на открытом ключе, постквантовая криптография, решетки, BKZ-алгоритм.

Keywords: public key cryptography, post-quantum cryptography, lattice, BKZ algorithm.

Введение

Решеточные криптосистемы появились в 1990-е гг. 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 решеток, мешающая злоумышленнику вскрыть зашифрованное сообщение, является предположительно устойчивой к атакам, выполняемым на квантовых компьютерах при использовании соответствующих алгоритмов [1].

В частности, неподдельный интерес в среде криптографов вызвала криптосистема NTRU, представленная Дж. Хоффштейном, Дж. Пайфер и Дж. Х. Сильверманом около 1996 г. Эта криптосистема среди прочих постквантовых обещала более короткие ключи и оптимальную

Вестник Балтийского федерального университета им. И. Канта.
Сер.: Физико-математические и технические науки. 2020. № 4. С. 16 – 25.

производительность. Однако проблема однозначного расшифрования сообщения так и не была решена: сообщение с исчезающе малой, но все же ненулевой вероятностью могло не зашифроваться на данном ключе [1]. Также, несмотря на оптимальность производительности по сравнению с конкурирующими постквантовыми решениями, NTRU все же страдала неоптимизованностью. Именно поэтому в августе 2017 г. в статье [2] группа исследователей привела «готовый к практическому применению» вариант NTRU под названием NTRU Prime. Главными достижениями их подхода стали сокращенная длина ключа, оптимизированная производительность и гарантия возможности расшифровки сообщения. Однако ценой такого выигрыша является потенциально «растянутый» (англ. overstretched) параметр q, что может привести к возможной уязвимости к атакам с использованием подрешеток малого ранга, как это описано в [3].

Цель нашего исследования — реализация оптимизированного алгоритма поиска параметров BKZ-алгоритма β и размерности k подрешетки, к которой применяется BKZ-алгоритм, для дальнейшего использования при взломе криптосистем, в основу которых положена сложность проблемы нахождения кратчайшего вектора в так называемых NTRU-решетках [5].

Актуальность данной работы заключается в новизне предложенного алгоритма подбора оптимальных параметров (k, β) для редукции решетки с использованием BKZ-алгоритма (далее — BKZ-редукции), обеспечивающих наибольшую скорость ее выполнения.

Основные понятия

Пусть $v_1, ..., v_n \in R^m$ — множество линейно независимых векторов. Множество $\mathcal{L}$ их комбинаций с целочисленными коэффициентами называется решеткой, порожденной этими векторами. Иными словами,

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

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

Пусть $v_1, ..., v_n \in \mathbb{R}^m$ — базис решетки $\mathcal{L}$. Определим векторы $w_i = a_{i_1} v_1 + \ldots + a_{i_n} v_n, 1 \leqslant i \leqslant n,$ принадлежащие $\mathcal{L}$. Коэффициенты $a_{i,j}$, где $1 \leqslant i, j \leqslant n,$ целочисленны по определению решетки. 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 решетки $\mathcal{L}$ связаны между собой целочисленными матрицами с определителем, равным ±1 [1].

Решетка $\mathcal{L}$, базисные векторы которой образуют строки или столбцы следующей матрицы:

$$B = \begin{pmatrix} q \cdot I_n & 0 \\ h & I_n \end{pmatrix},$$

где h — матрица размерности $n \times n$, называется NTRU-решеткой [4].

Криптостойкость решетчатых криптосистем, использующих NTRU-решетки, основывается на сложности задачи **SVP** (поиска кратчайшего вектора). Она заключается в отыскании такого вектора $w \in \mathcal{L}(v_1, \ldots, v_n) \setminus \{0\}$, что его норма минимальна.

Методы

В ходе работы расмотренно уравнение

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

выведенное в статье [2], связывающее параметры n, q NTRU-решетки и необходимые для BKZ-редукции, описанной в той же статье, параметры k, β. Так как меньшие параметры k и β ведут к ускорению выполнения алгоритма, ставится задача нахождения наименьшего β и наименьшего k, удовлетворяющих (1) при выбранном β.

Данное уравнение проанализированно численными методами и решено методом бинарного поиска сначала по переменной β, а затем — по переменной k. Реализация алгоритма осуществлена в системе компьютерной алгебры Sage 9.1.

Ядро алгоритма состоит из двух циклов: по переменной β и вложенного цикла по переменной k. Внешний цикл работает по принципу бинарного поиска: множество поиска разбивается на две части, причем заведомо известно, что существует число β_0 такое, что для всех $\beta < \beta_0$ не существуют решения (1) такие, что $\beta \leqslant 2k \leqslant 2n$. Внутренний цикл тоже работает по принципу бинарного поиска, но ищется локальный максимум функции

$$\mathcal{D}(\beta, k) = \delta_\beta - \sqrt[k(3k-1)]{\left(\frac{k}{2\pi e}\right)^{k/2} \cdot q^k \cdot (n/2)^{-n}}$$

при помощи метода «ходьбы в гору»: множество поиска разбивается на две части (левую и правую) с пограничным элементом k_0. После этого высчитываются $\mathcal{D}(\beta, k_0 - 1)$ и $\mathcal{D}(\beta, k_0 + 1)$. Если первое значение больше, то выбирается левая часть, в противном случае — правая.

Исходный код программы размещен по ссылке: https://github.com/alexgit256/Diploma-NTRU-attack-params-BKZ-/blob/main/Optimal%20BKZ%20params%20finder.py.

Для иллюстрации зависимости параметров k, β от n и $\log q$ приведены соответствующие графики для случаев n = 128, 256, 384, 512, 640, 768, 896, 1024 (см. рис. 1—16). Все логарифмы берутся по основанию 2, если не указано иное.

Результаты

По итогам исследования был разработан алгоритм поиска параметров k, β, доступный по приведенной выше ссылке. Так как сложность бинарного поиска во множестве из n элементов оценивается как $O(\log n)$, сложность данного алгоритма равна $O(\log^2 n)$.

Ниже представлены графики зависимости β и k от $\log q$ для фиксированных значений n = 128, 256, 384, 512, 640, 768, 896, 1024 (рис. 1—16):

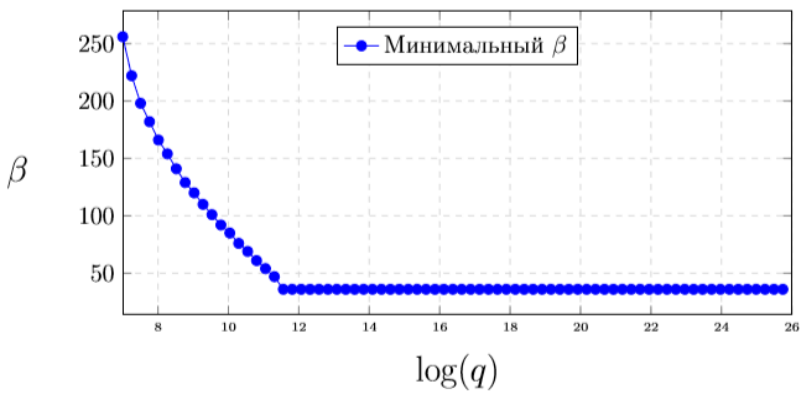

Рис. 1. График зависимости β от $\log q$ при n = 128

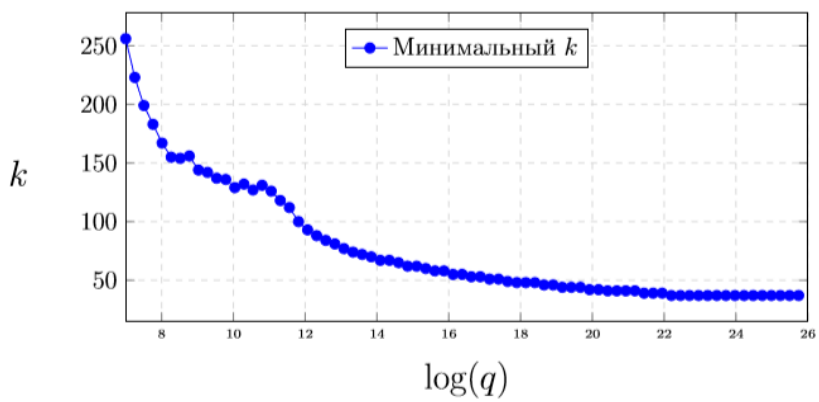

Рис. 2. График зависимости k от $\log q$ при n = 128

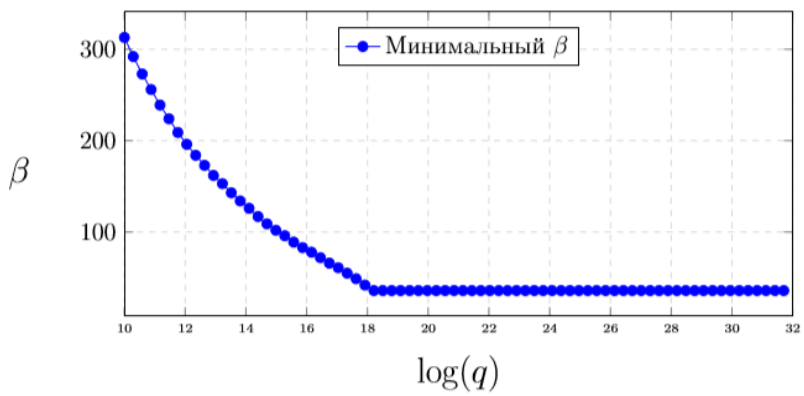

Рис. 3. График зависимости β от $\log q$ при $n = 256$

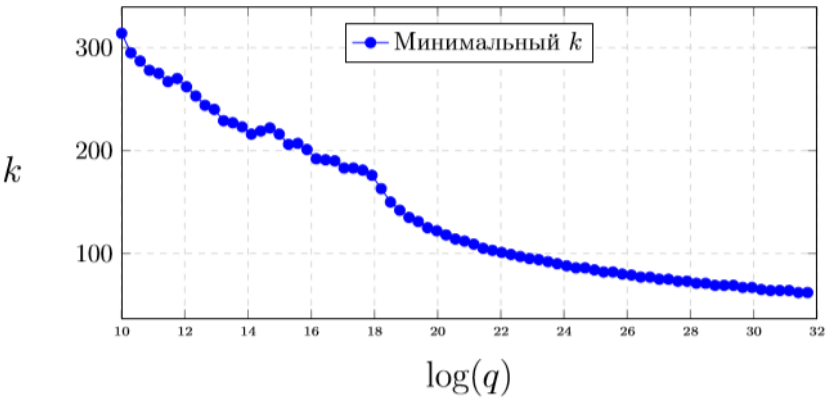

Рис. 4. График зависимости k от $\log q$ при $n = 256$

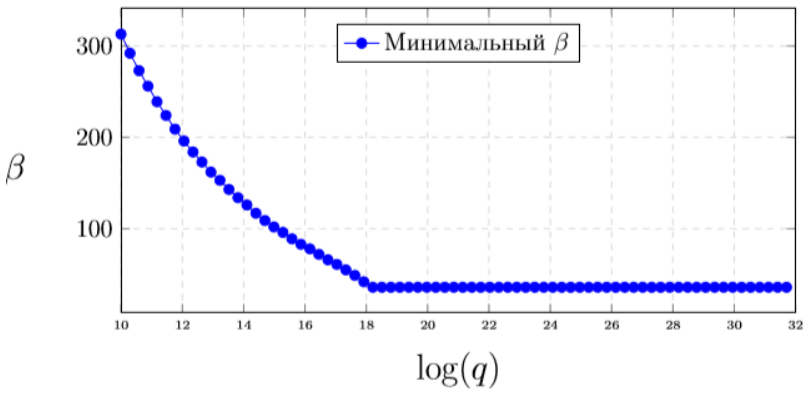

Рис. 5. График зависимости β от $\log q$ при $n = 384$

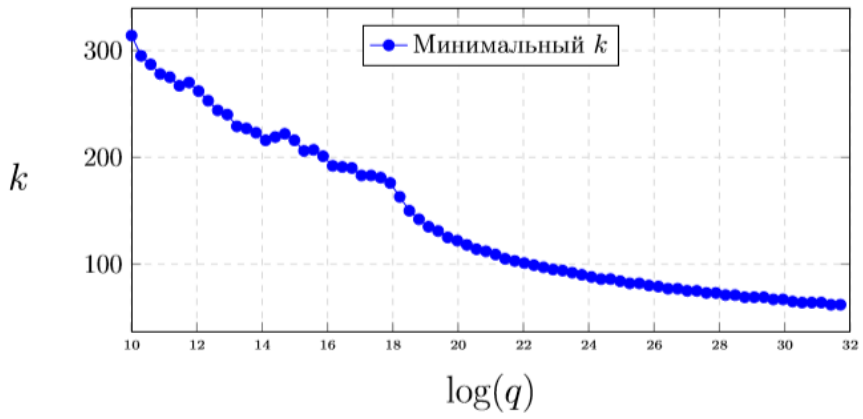

Рис. 6. График зависимости k от $\log q$ при $n = 384$

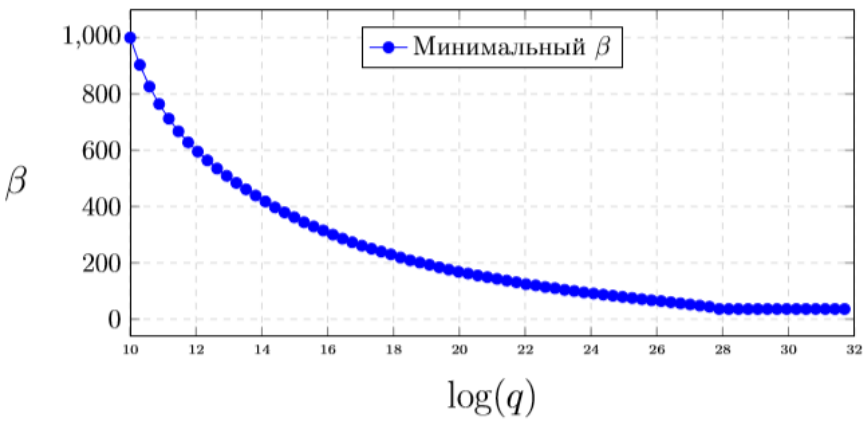

Рис. 7. График зависимости β от $\log q$ при $n = 512$

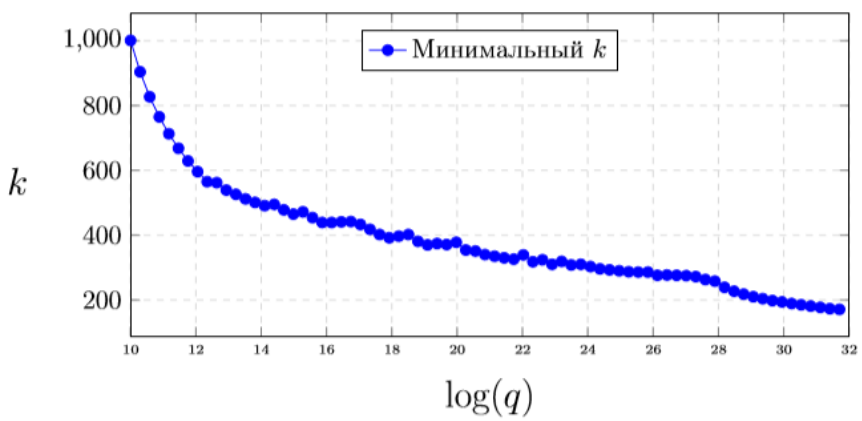

Рис. 8. График зависимости k от $\log q$ при $n = 512$

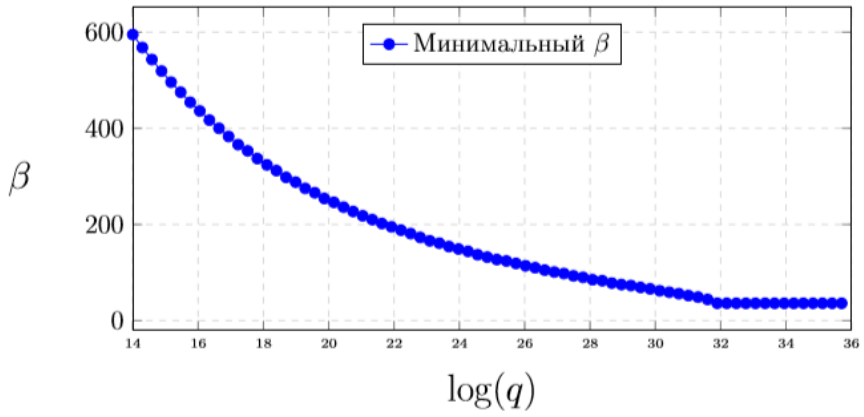

Рис. 9. График зависимости β от $\log q$ при $n = 640$

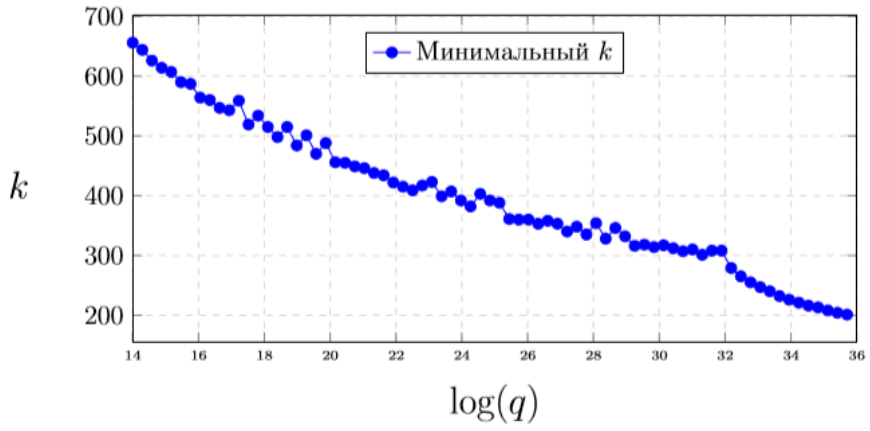

Рис. 10. График зависимости k от $\log q$ при $n = 640$

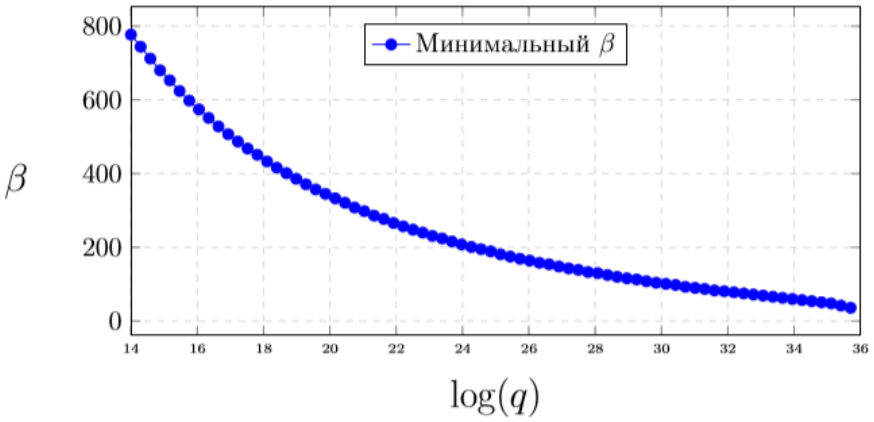

Рис. 11. График зависимости β от $\log q$ при $n = 768$

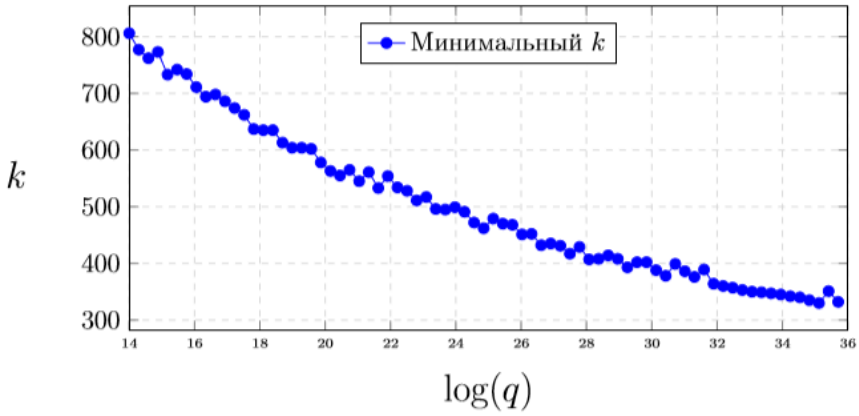

Рис. 12. График зависимости k от $\log q$ при $n = 768$

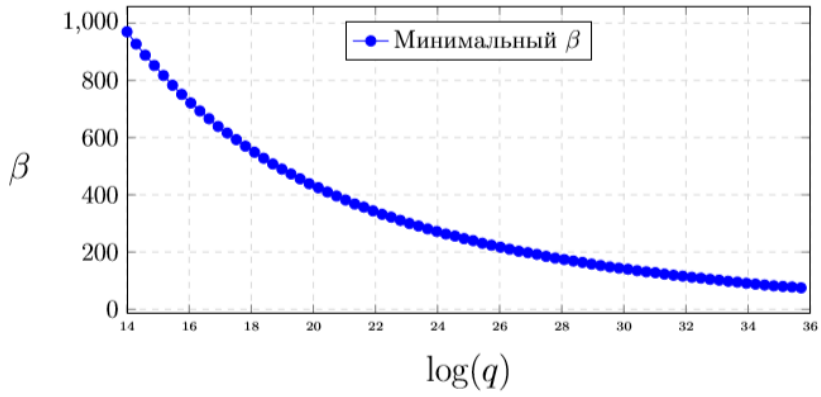

Рис. 13. График зависимости β от $\log q$ при $n = 896$

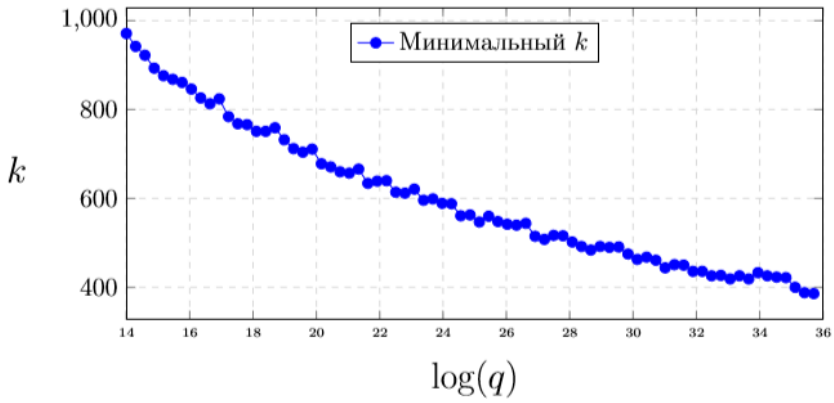

Рис. 14. График зависимости k от $\log q$ при $n = 896$

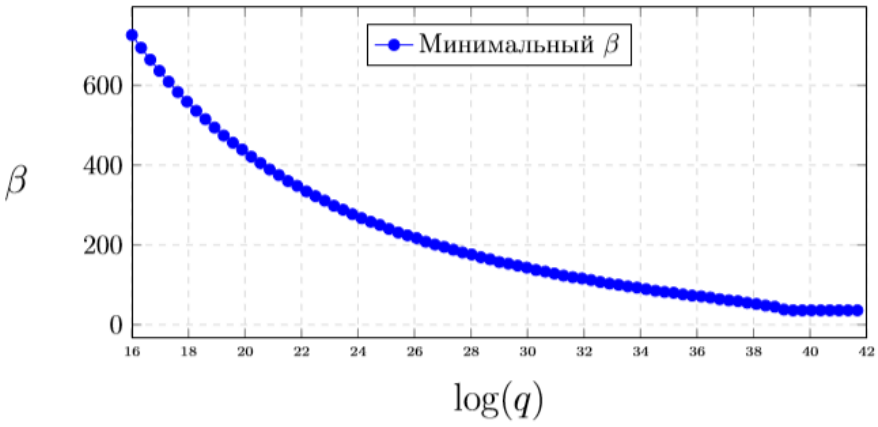

Рис. 15. График зависимости β от $\log q$ при $n = 1024$

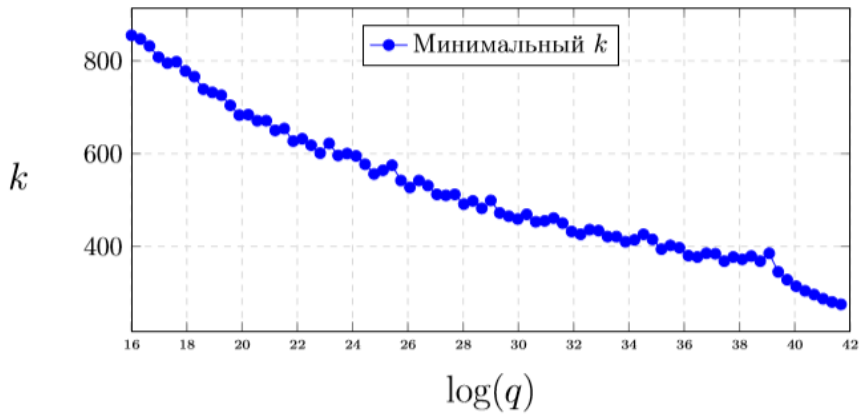

Рис. 16. График зависимости k от $\log q$ при $n = 1024$

Заключение

По итогам проведенного численного исследования был проверен результат [2], заключающийся в том, что модуль $q \approx 2^{\sqrt{n}}$ не является безопасным и ведет к возможности успешной атаки методом BKZ-редукции. Сложность проведения BKZ-редукции монотонно убывает с ростом $\log q$ что обусловленно убыванием параметра β, от которого зависит сложность атаки [2].

Интересным вопросом остается значение β, достаточное для успешной атаки на практике. Приведенное в [2] уравнение дает лишь верхнюю оценку для β, k, тогда как на деле атака может быть успешной и при немного меньших значениях этих параметров. Для этого следует провести численные эксперименты BKZ-редукции NTRU-решеток согласно методологии, описанной в [6], и сравнить их с результатами, выдаваемыми алгоритмом, предложенным в нашей статье.

Список литературы

1. *Hoffstein J., Pipher J., Silverman J.H.* An Introduction to Mathematical Cryptography. Springer, 2014.

2. *Bernstein D.J., Chuengsatiansup Ch., Lange T., van Vredendaal Ch.* NTRU Prime: reducing attack surface at low cost. URL: https://eprint.iacr.org/2016/461.pdf (дата обращения: 15.10.2020).

3. *Lee Ch., Wallet A.* Lattice analysis on MiNTRU problem. URL: https://www.semanticscholar.org/paper/Lattice-analysis-on-MiNTRU-problem-Lee-Wallet/d922d602c196bebb2057b734fd8012b1bbb3cb9a (дата обращения: 15.10.2020).

4. *Monteverde M.* NTRU software implementation for constrained devices. Leuven, 2007.

5. *Micciancio D., Voulgaris P.* Faster exponential time algorithms for the shortest vector problem // 21st Annual ACM-SIAM Symposium on Discrete Algorithms. Austin, 2010. P. 1468—1480.

6. *Chen Yu.* Réduction de réseau et sécurité concrete du chiffrement completement homomorphe : PhD Thesis. P., 2013.

Об авторе

Александр Сергеевич Каренин — студент, Балтийский федеральный университет им. И. Канта, Россия.

E-mail: tremeloesalex@gmail.com

The author

Alexander S. Karenin, Student, Immanuel Kant Baltic Federal University, Russia.

E-mail: tremeloesalex@gmail.com