Отчёт по заявке

“Алгоритмы нахождения коротких векторов в алгебраических решетках”

Елена Киршанова

15 декабря 2022 г.

Содержание

1 Результаты

1.1 Публикации прошлогодних работ

В отчете прошлого года была упомянута статья, опубликованная в этом году на ACM Conference on Computer and Communications Security (CCS).

1. Shweta Agrawal, Elena Kirshanova, Damien Stehlé, Anshu Yadav. *Practical, Round-Optimal Lattice-Based Blind Signatures*. ACM CCS 2022.
   Полная версия доступна по адресу: `https://eprint.iacr.org/2021/1565`.

1.2 Результаты 2022 года

1.2.1 Опубликованные результаты со ссылкой на грант

[1] Jean-François Biasse, Xavier Bonnetain, Elena Kirshanova, Andre Schrottenloher, Fang Song. Quantum algorithms for attacking hardness assumptions in classical and post-quantum cryptography. Journal IET Information Security. `https://doi.org/10.1049/ise2.12081`

Полная версия доступна по адресу: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.1049/ise2.12081

[2] Elena Kirshanova, Alexander May. Decoding McEliece with a Hint – Secret Goppa Key Parts Reveal Everything. Security and Cryptography for Networks: 13th International Conference, SCN 2022, Amalfi (SA), Italy, September 12–14, 2022, Pages 3–20. https://doi.org/10.1007/978-3-031-14791-3_1
Полная версия доступна по адресу: https://eprint.iacr.org/2022/525.pdf

1.2.2 Результаты на рецензии

1. [KMN] Elena Kirshanova, Alexander May, Julian Nowakowski. Attacking NTRU in Practice: Cyclotomic Ring, Almost-Parallel Hints, and Sieving. Статус: на резенции (конференция PKC 2023).

1.3 Обзор результатов 2022 года

1. **Монография о пост-квантовой сложности криптографических задач**. В работе [1] Е.Киршанова совместно с соавторами представили обзорную статью об алгоритмах (и их квантовых ускорениях) решения трудных задач, лежащих в основе пост-квантовых криптосистем, в частности, систем на решетках и кодах. Проведен полный обзор современных алгоритмов и их сравнительный анализ сложности. В статье Киршанова ответсвенна за Главу 8 “Евклидовы решетки” и Главу 9 “Предположения сложности на кодах”. Киршановой проведена систематизация всех известных алгоритмов (классических и квантовых) для трудных задач на решетках и кодах. Описаны открытые вопросы и направления научных исследований по этим темам. В других главах описывются основы квантовых алгоритмов, представлен анализ алгоритма Шорра, описаны квантовые алгоритмы взлома симметричных схем, а также приведен разбор алгоритов решения задач на изогениях (еще одно пост-квантовое направление криптографии).

2. **Атаки на криптосистему McEliece**. Совместно с проф. А. Майем была опубликована статья “Decoding McEliece with a Hint - Secret Goppa Key Parts Reveal Everything” [2]. В статье рассматривается атака на секретный ключ криптосистемы МакЭлис (в частности, рассматриваются параметры версии Classic McEleice – кандидата на стандартизацию NIST). Конкретно, в работе анализируется необходимое число известных бит секретного ключа для восстановления *всех* бит секретного ключа (такие атаки носят название Partial Key Recovery attacks). Это одна из немногих атак на криптосистему McEliece, использующая структуру кода Гоппы – кода, лежащего в основе криптосистемы. Мы продемонстрировали, что “избыточность” кода Гоппы может быть использована для восстановления всех бит секретного ключа по всего-лишь 25% известных бит. Атака реализована в системе Sage, код доступен по адресу https://github.com/ElenaKirshanova/leaky_goppa_in_mceliece. Представленный алгоритм эффективен и работает за несколько секунд на ноутбуке.

3. **Практические атаки на NTRU [KMN]**. Основная атака на криптосистемы семейства NTRU – атака с использованием редукции (публичного) базиса решетки, полученного из открытого ключа криптосистемы. В нашей работе мы предлагаем набор инструментов для атаки современных версий NTRU: мы определяем несколько решеток, короткий вектор (или короткие вектора) в каждой из которых дает информацию о секретном ключе (в нашем случае мы восстанавливаем секретный ключ полностью). Далее, на каждой

из предложенных решеток мы запускаем алгоритм блочной редукции базиса (BKZ) и смотрим, какая из решеток более выгодна на практике, т.е. выдает секретный вектор за меньшее число "шагов" (более строго метрика успеха сформулирована в статье).

Использование кастомизированного алгоритма редукции на предлагаемых нами решетках позволило нам взломать NTRU-HPS и NTRU-HRSS параметры в размерностях 171 и 211 соответственно. NTRU-HPS/NTRU-HRSS – версии криптосистемы NTRU, предложенные к стандартизации пост-квантовых примитивов NIST. На сегодняшний момент это первый результат, достигающий взлома NTRU в таких размерностях. Конструкция новых решеток (в статье мы их называем циклотомическими проективными решетками) позволила нам ускорить атаку и получить первые практические результаты для современных версий NTRU.

Этот результат напрямую связан с задачей нахождения коротких векторов в алгебраических решетках, так как задача NTRU есть ни что иное, как нахождение короткого (псевдо) базиса в модуях ранга 2 над кольцом целых циклотомических полей.

Помимо криптографически ориентированных результатов, совмесно с коллегой Малыгиной Е.С. Киршанова работает над конструкцией плотной решетки из подполевых подкодов кодов башни Гарсии-Штихтенота (статья Serge Vlăduţ "Lattices with exponentially large kissing numbers", `https://arxiv.org/abs/1802.00886` стала отправной точкой для этой работы). В настоящий момент ведётся работа по получению эффективного алгоритма декодирования подполевых подкодов башни Гарсии-Штихтенота. Предполагается использовать подход "мягкого" декодирования, позволяющий модифицировать декодер для кода Рида-Соломона к его подполевому подкоду – БЧХ-коду. Мы полагаем, что такая модификация применима и на АГ-коды. Черновик работы с описанием плотной подрешетки доступен по адресу `https://www.overleaf.com/read/zjyxbgcjjrtm`

1.4 Обзор результатов 2020-2021 года

За предыдущие два года Киршановой Е.А. были получены следующие результаты:

- **Алгоритм нахождения образующих идеала Штикельбегера мультиквадратичных полей.** В работе рассматриваются мультиквадратичные поля $\mathrm{K} = \mathbf{Q}(d_1, d_2, \ldots, d_n)$, где $d_i = 1 \mod 4$ свободны от квадратов и попарно взаимно просты. Предлагается алгоритм вы- числения идеала Штикельбергера поля K. Такой алгоритм интересен, в первую очередь, с точки зрения вычислений группы классов поля K.

  Е.Киршанова, Е.Малыгина, С.Новосёлов, Д.Олефиренко. *Алгоритм вычисления идеала Штикельбергера для мультиквадратичных полей.* Prikl. Diskr. Mat., 2021, no. 51, 9–30. Полная версия доступна по адресу: `https://crypto-kantiana.com/elena.kirshanova/Papers/kirshanova_pdm.pdf`

- **Нахождение нижней границы для задачи поиска ближайшего соседа и её криптоанализ пост-квантовых схем на решётках и кодах**.

  В работе доказываются нижние границы для поиска ближайшего соседа (Nearest Neighbour Search) в контексте алгоритмов просеивания для решения задачи нахождения короткого вектора методов, то есть нахождение ближайшего соседа в евклидовой метрики и для решения задачи декодирования линейного кода в метрике Хэмминга. Для евклидовой метрики в работе показано, что для случайных векторов, равномерно распределённых на единичной сфере, алгоритм поиска ближайшего соседа, основанный на сферических

фильтрах [Becker–Ducas–Gama–Laarhoven, SODA 2016], оптимален. Для метрики Хэмминга показаны новые нижние границы для алгоритмов декодирования случайных линейных кодов, использующих поиск ближайшего соседа [May–Ozerov, Eurocrypt 2015].

E.Kirshanova, T.Laarhoven Lower bounds for nearest neighbor searching and post-quantum cryptanalysis. Crypto 2021.
Полная версия доступна по адресу: `https://crypto-kantiana.com/elena.kirshanova/Papers/lowerbounds.pdf`

- **Комбинаторые атаки на задачу NTRU**. Совместно с Iggy van Hoof и Alenxander May, мы представляем квантовые ускорения для алгоритмов решения задачи NTRU. Точнее, основываясь на классической комбинаторной атаке A.May "How to meet ternary LWE keys", мы предлагаем квантовую версию этой атаки, а также конкретную битовую сложность параметров криптосистем, основанных на тренарной версии LWE (задача NTRU является частным случаем тернарого LWE).

  Совместно с Alexander May мы предлагаем также классическое ускорение для комбинаторного алгоритма решения задачи тренарной версии LWE.

  1. Iggy van Hoof, Elena Kirshanova, Alexander May. *Quantum Key Search for Ternary LWE.* PQCrypo2021. Lecture Notes in Computer Science 2021, no. 12841 Полная версия доступна по адресу: `https://eprint.iacr.org/2021/865`
  2. Elena Kirshanova, Alexander May. *How to Find Ternary LWE Keys Using Locality Sensitive Hashing.* International Congerence on Cryptography and Coding. Lecture Notes in Computer Science 2021, no. 13129.
     Полная версия доступна по адресу: `https://eprint.iacr.org/2021/1255`

- **Конструкции слепой подписи.** Совместно с Shweta Agrawal, Damien Stehlé, Anshu Yadav мы предлагаем первую эффективную слепую подпись на решетках (и вообще, первую эффективную *пост-квантовую* слепую подпись). Трудная задача, лежащая в основе безопасности схемы – модификация задачи нахождения короткого целочисленного решения (Short Integer Solution, SIS). Модификация называется one-more-ISIS – это аналог задач one-more-RSA или one-more-CDH в доквантовых конструкциях слепых подписей. Так как в этой статье впервые формулируется эта задача, она должна быть тщательно проанализирована.

  Shweta Agrawal, Elena Kirshanova, Damien Stehlé, Anshu Yadav. *Practical, Round-Optimal Lattice-Based Blind Signatures.* ACM CCS 2022.
  Полная версия доступна по адресу: `https://eprint.iacr.org/2021/1565`.

2 Участие в конференциях

1 `Тема:` Decoding McEliece with a Hint - Secret Goppa Key Parts Reveal Everything
`Место:` Конференция SCN (Италия, Амальфи), сентябрь 2022
`Слайды` `https://crypto-kantiana.com/elena.kirshanova/talks/Talk_SCN.pdf`

2 `Тема:` Decoding McEliece with a Hint
`Место:` ACCESS Seminar, ноябрь 2022
`Слайды` `https://sites.google.com/view/access-seminar`

3 Тема: Blind Signatures

Место: Круглый стол PQNet https://www.sofiaceli.com/PQNet-Workshop/

Дата: 27.11.22

Слайды https://crypto-kantiana.com/elena.kirshanova/talks/Talk_BsigPQNet.pdf

3 Иная научная деятельность

- Программный комитет международных конференций
  – PQCrypto 2022 https://2022.pqcrypto.org/,
  – ANTS XV https://people.maths.bris.ac.uk/~jb12407/ANTS-XV/index.html,
  – AsiaCrypt 2022 https://asiacrypt.iacr.org/2022/.
- Научный комитет, лектор, организатор летней школы "Aspects mathématiques de la cryptographie post-quantique". Рабат, Марокко. Октябрь 2023
- Работа руководителем по гранту РНФ-DFG совместно с Prof.Dr. Alexander May (Рурский университет г. Бохум) на тему "Криптоанализ пост-квантовых примитивов, основанных на решётках и кодах: рекорды на практике и ускорения в теории".
- Работа по подготовке стандарта пост-квантовых схем цифровой подписи и шифрования на решетках совместно с https://qapp.tech/

4 Педагогическая деятельность

- Веденииа "Криптография на решетках" для специальности Компьютерная безопасность Института физики, математики и информационных технологий БФУ им. И.Канта. Материалы курса по адресу https://crypto-kantiana.com/elena.kirshanova/teaching/lattices_2022.html
- Ведение курса "Теория кодирования и сжатия информации" для специальности Компьютерная безопасность Института физики, математики и информационных технологий БФУ им. И.Канта. Материалы курса по адресу https://crypto-kantiana.com/elena.kirshanova/teaching/coding_theory_2022.html
- Ведение курса "Информационная безопасность" для магистратуры Института Физики, Математики и Информационных технологий БФУ им. И.Канта. Материалы курса по адресу https://crypto-kantiana.com/elena.kirshanova/teaching/info_sec_2022.html
- Разработка и ведение курса повышения квалификации "Введение в кибербезопасность" https://lms-3.kantiana.ru/course/view.php?id=11814
- Руководство дипломными работами (специальность "Компьютерная безопасность" БФУ им. И.Канта) по темам
  – Исследование решёток, возникающих в алгоритмах исчисления индексов для решения дискретного логарифма (студент Можаев Александр, дата зашиты 20.01.23)
  – Трудность задачи декодирования случайных тернарных кодов (студент Иванов Артём, дата зашиты 20.01.23)
- Руководство аспирантом Карениным А.С. Тема диссертации "Алгоритмы нахождения короткого вектора в алгебраических решетках".