Отчёт по заявке

“Алгоритмы нахождения коротких векторов в алгебраических решетках”

Елена Киршанова

14 декабря 2020 г.

Содержание

1 Результаты

1. **Алгоритм нахождения образующих идеала Штикельбегера мультиквадратичных полей.**

   Получение идеала Штикельбергера в явном виде является важной алгоритмической задачей в вычислительной теории чисел, в теории групп классов и, с недавних пор, в криптоанализе. Для числового поля K идеал Штикельбергера I – идеал групповой алгебры $\mathbb{Z}[G_K]$, где $G_K = \mathrm{Gal}(K/\mathbb{Q})$ – группа Галуа поля K. Полезное свойство I заключается в том, что под действием элементов I на Cl_K – группу классов идеалов K – любой класс становится тривиальным классом (иначе говоря, J^σ – главный идеал для любого $\sigma \in I$ и любого идеала J кольца целых $\mathcal{O}_K$ числового поля K).

   В работе рассматриваются мультиквадратичные поля вида $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \ldots, \sqrt{d_n})$, где $d_i \equiv 1 \bmod 4$ свободны от квадратов и попарно взаимно просты. Предлагается алгоритм вычисления идеала Штикельбергера поля K. Такой алгоритм интересен, в первую очередь, с точки зрения вычислений группы классов поля K. В криптографии эта задача возникает в конструкциях проверяемых функций задержки (VDF) (Pietrzak K., Simple verifiable delay functions, ITCS 2019)и в гомоморфном шифровании (Pedrouzo-Ulloa A., Troncoso-Pastoriza J. R., Gama N., Georgieva M., Pérez-González F.Revisiting Multivariate Ring Learning with Errors and its Applications on Lattice-based Cryptography //IACR Cryptol. ePrint Arch. 2019/1109).

   Алгоритм, описанный в статье, имеет сложность $\mathcal{O}(\lg \Delta_K \cdot 2^n \cdot \mathrm{poly}(n))$, где Δ_K — дискриминант K. Таким образом, он является полиномиальным от степени расширения $[K : \mathbb{Q}] = 2^n$ и име-

ет логарифмическую зависимость от дискриминанта поля. В основе алгоритма лежит работа Кучеры [Journal of number theory 56, 1996].

Реализация алгоритма представлена в открытом доступе[1]

Тезис статьи представлен на трудах конференции SibeCrypt2020 [2]. Полная версия работы отправлена в журнал "Прикладная дискретная математика" [1].

2. **Разработка предложения к стандартизации пост-квантовой схемы цифровой подписи на решётках.**

   Криптографические примитивы на решётках – одно из самых обещающих направлений современной криптографии не только ввиду стойкости этих примитивов к атакам на квантовом компьютере, но и вследствие большого спектра конструкций (гомоморфное шифрование, электронные голосования, различные типы подписей), а также их надежности к классическим атакам. Криптографические конструкции на решетках не только элегантны в теории, но значимы на практике, и имеют большие шансы стать стандартами в ближайшее время. [2]

   В работе представлена схема цифровой подписи, основанная на алгебраических решётках. Доказательство безопасности схемы основано на парадигме Фиата-Шамира (Fiat-Shamir, How to prove yourself: Practical solutions to identification and signature problems, Crypto'96) и по идеологии продолжает серию работ по предложению конкретных схем подписи (L.Ducas, E.Kiltz, T.Lepoint, V.Lyubashevsky, P.Schwabe, G.Seiler, D.Stehle. Crystals-dilithium: A lattice-based digital signature scheme, CHES'18). Основное отличие нашей схемы от ранее предложенных заключается в том, что безопасность ключей основана на так называемой задаче Lenarning With Rounding (LWR), а не на задаче Learning With Erros (LWE). Мы считаем, что наш подход упрощает описание и потенциально ускоряет вычисления.

   Исследование проводится в рамках Рабочей группы ТК 26 "Постквантовые криптографические механизмы".

   Предварительные результаты работы представлены в [3]. Открытый код можно найти по адресу `https://github.com/ElenaKirshanova/pqc_LWR_signature`
   Работа находится на стадии разработки, в следующем году планируется провести аналогичную работу по теме шифрования с открытым ключом на решётках.

3. **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. А значит, современные эффективные алгоритмы просеивания, использующие сферические фильтры как метод поиска ближайшего соседа, не получится улучшить за счет использования другого метода. Следовательно, асимптотическая сложность алгоритмов просеивания, используемая для вычисления криптографической стойкости конкретных параметров, является оптимальной для этого семейства алгоритмов.

   Для метрики Хэмминга показаны новые нижние границы для алгоритмов декодирования случайных линейных кодов, использующих поиск ближайшего соседа [May–Ozerov, Eurocrypt 2015].

[1] `https://gitlab.com/DenisOl/stickelberger-ideal`

[2] За процессом стандартизации пост-квантовых механизмов в США можно проследить по адресу `https://csrc.nist.gov/projects/post-quantum-cryptography`

Отсюда мы делаем вывод, что источник для улучшения современных алгоритмов декодирования, необходимо искать не в улучшении методики поиска ближайшего соседа.

Оба результата, для евклидовой метрики и для метрики Хэмминга, имеют важное значение для выбора параметров криптосистем на решетках и кодах, так как затрагивают самые эффективные из известных алгоритмов (атак). Наличие нижних границ сложности таких алгоритмов даёт уверенность в том, что для изменения криптографической стойкости выбранных параметров, требуется кардинально новые методы криптоанализа.

2 Публикации

Список литературы

[1] Е.Киршанова, Е.Малыгина, С.Новосёлов, Д.Олефиренко.
АЛГОРИТМ ВЫЧИСЛЕНИЯ ИДЕАЛА ШТИКЕЛЬБЕРГЕРА ДЛЯ МУЛЬТИКВАДРАТИЧНЫХ ПОЛЕЙ.
Прикладная дискретная математика. Статус: на рецензировании.
Полная версия доступна по адресу: `https://crypto-kantiana.com/elena.kirshanova/Papers/kirshanova_pdm.pdf`

[2] Е.Киршанова, Е.Малыгина, С.Новосёлов, Д.Олефиренко.
АЛГОРИТМ ВЫЧИСЛЕНИЯ ИДЕАЛА ШТИКЕЛЬБЕРГЕРА ДЛЯ МУЛЬТИКВАДРАТИЧНЫХ ПОЛЕЙ.
Прикладная дискретная математика. Приложение.Труды конференции SibeCrypt2020.
Полная версия доступна по адресу: `https://crypto-kantiana.com/elena.kirshanova/Papers/stickelberger_ideal.pdf`

[3] Е.Киршанова, Н.Колесников, Е.Малыгина, С.Новосёлов.
ПРОЕКТ СТАНДАРТИЗАЦИИ ПОСТ-КВАНТОВОЙ ЦИФРОВОЙ ПОДПИСИ
Прикладная дискретная математика. Приложение. Труды конференции SibeCrypt2020
Полная версия доступна по адресу: `https://crypto-kantiana.com/main_papers/main_Signature.pdf`.

[4] E.Kirshanova, T.Laarhoven
LOWER BOUNDS FOR NEAREST NEIGHBOR SEARCHING AND POST-QUANTUM CRYPTANALYSIS
Статус: на рецензировании (EuroCrypt2021)
Полная версия доступна по адресу: `https://crypto-kantiana.com/elena.kirshanova/Papers/lowerbounds.pdf`

3 Участие в конференциях и школах

1 `Тема:` A k-List Algorithm for LWE

`Место:` Воркшоп “Lattices: Geometry, Algorithms and Hardness”, The Simons Institute for the Theory of Computing, Беркли, США

В рамках семестра “Lattices: Algorithms, Complexity, and Cryptography”

`Дата:` 19.02.20

`Аннотация:` В докладе были представлены несколько версий проблемы k-списков с заделом на их приложение в криптоанализе. Разобраны эвристические алгоритмы просеивания, так называемый алгоритм BKW для задачи обучения с ошибками и алгоритм Куперберга для решения

задачи Группы Классов Смежности Диэдральной группы.

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

Видео https://www.youtube.com/watch?v=VMkxcDT3D5w&list=PLgKuh-lKre12CuCYPwpfH77-K6U_3JweQ&index=7

2 Тема: Overview of Quantum Cryptanalysis of Lattice Systems

Место: Воркшоп "Quantum Cryptanalysis of Post-Quantum Cryptography", The Simons Institute for the Theory of Computing, Беркли, США

В рамках семестра "Lattices: Algorithms, Complexity, and Cryptography"

Дата: 22.02.20

Аннотация: I this talk I will explain a way to analyse sieving algorithms both in their classical and quantum versions.

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

Видео https://simons.berkeley.edu/talks/overview-quantum-cryptanalysis-lattice-systems

3 Тема: Sieving in practice: The Generalized Sieve Kernel (G6K)

Место: Онлайн семинар. Беркли, США

В рамках семестра "Lattices: Algorithms, Complexity, and Cryptography"

Дата: 05.05.20

Аннотация: In this talk I will explain the way sieving algorithms are implemented in the Generalized Sieve Kernel(G6K) – an open-source implementation of the currently fastest sieve in practice. I will talk about the Nguen-Vidick sieve algorithm, tuple sieve, and the way these algorithms can be sped up with locality-sensitive hashing, as well about several tricks that allowed to improve the performance of the implementation.

Слайды https://crypto-kantiana.com/elena.kirshanova/talks/talk_g6k.pdf

Видео https://www.youtube.com/watch?v=rRhoJe-6bWA&list=PLgKuh-lKre101qeibKuHS1chgHzIahf7m&index=2

4 Тема: Пост-квантовые криптосистемы на решетках и кодах

Место: Онлайн Семинар "Индустриальная математика", СПбГУ, Санкт-Петербург, Россия

Дата: 09.06.20

Аннотация В своём докладе я расскажу о построении криптографических примитивов с открытым ключом, сложность которых основана на задачах в евклидовых решётках и в кодах. Мы сформулируем эти "трудные" задачи, рассмотрим существующие алгоритмы их решения и методы построения шифрования на примере кандидатов к стандартизации NIST (Национальное бюро стандартов США). Мы поговорим о том, как осуществляется криптоанализ систем на решётках и кодах, и сравним их производительность с существующими стандартами. В докладе я буду предполагать от слушателя базовые знания линейной алгебры, основы теории вероятности и теории сложности.

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

Видео https://sites.google.com/view/industrial-math-seminar/past?authuser=0#h.p_98LJ_Y7XxOs4

5 Тема: Quantum speed-ups for sieving algorithms for the shortest vector problem

Место: Офф-лайн конференция "15th Conference on the Theory of Quantum Computation, Communication and Cryptography", Рига, Латвия

Дата: 11.06.20

Аннотация Аннотация к статье https://crypto-kantiana.com/elena.kirshanova/Papers/quantum_sieving.pdf

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

Видео https://www.youtube.com/watch?v=Y0gdvvzuADY

6 Тема: Open questions in lattice-based cryptanalysis

Место: Офф-лайн воркшоп "on the Mathematics of Post-Quantum crypto", Окланд, Новая Зеландия

Дата: 07.07.20

Аннотация In this talk I'll give a list of my favourite open problems that concern algorithms (classical and quantum) for hard lattice problems. Topics I aim to discuss are targeted towards cryptanalysis of post-quantum lattice-based primitives and include: the shortest vector problem for ℓ_∞. norm, combinatorial algorithms for the LWE problem, potential venues to explore quantum hardness of LWE.

Слайды https://crypto-kantiana.com/elena.kirshanova/talks/ANTS20_Kirshanova.pdf

7 Тема: Цифровая подпись на алгебраических решётках

Место: Онлайн встреча участников Рабочей группы «Постквантовые криптографические механизмы» Москва, Россия

Дата: 20.10.20

Аннотация Был представлен черновик проекта цифровой подписи на решетках. https://crypto-kantiana.com/elena.kirshanova/talks/Gooseberry_20_10.pdf

8 Тема: Криптография на решётках: трудные задачи и конструкции

Место: Семинар "Математические методы криптографического анализа"Москва, Россия

Дата: 16.11.20

Аннотация В докладе рассказано о методах построения криптографических примитивов с открытым ключом, сложность которых основана на задачах в евклидовых решётках. Кроме этого, сформулированы эти "трудные" задачи, рассмотрены существующие алгоритмы их решения и методы построения цифровой подписи.

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

4 Работа в научных центрах и международных группах

- Совместная работа с D.Stehle и H.Kalachi (ENS Lyon, Франция) над сложностью задачи нахождения короткого вектора в метрике ℓ_∞ (публикация в процессе подготовки).
- Совместная работа с D.Stehle и H.Nguyen над сложностью задачи LWE и SIS (задачи "в среднем" на решётках) над кольцом целых чисел. (публикация в процессе подготовки).
- Совместная работа с A.May (Ruhr University Bochum, Германия) над практическим криптоанализом криптосистемы NTRU (публикация в процессе подготовки).

5 Педагогическая деятельность

- Разработка нового курса “Введение в криптографию” для магистров Института физики, математики и информационных технологий БФУ им. И.Канта
  Материалы и видео-лекции доступны по адресу `https://crypto-kantiana.com/elena.kirshanova/teaching/info_sec_2020.html`
- Разработка и ведение курса “Теория кодирования и сжатия информации”, БФУ им. И.Канта
  Материалы курса по адресу `https://crypto-kantiana.com/elena.kirshanova/teaching/coding_theory_2020.html`
- Разработка и ведение летней практики “Инструменты научно-исследовательской работы”, БФУ им. И.Канта
  Материалы курса по адресу `https://crypto-kantiana.com/elena.kirshanova/teaching/science_tools_2020/`
- Руководство дипломными работами (специальность “Компьютерная безопасность” БФУ им. И.Канта) по темам
  - Разработка системы электронного голосования (студент Д.Клинов, оценка “отлично”, январь 2020)
  - Гибридная атака на задачу Learning With Errors (LWE) с разряженным секретом: асимптотический анализ и реализация (студент М.Мищенко, дата защиты: январь 2021)
  - Атака на решетчатые криптосистемы с подрешетками малого ранга: асимптотический анализ и конкретная сложность (студент А.Каренин, дата защиты: январь 2021)