Отчёт по заявке

“Алгоритмы нахождения коротких векторов в алгебраических решетках”

Елена Киршанова

14 декабря 2021 г.

Содержание

1 Результаты

1.1 Публикации прошлогодних работ

1. Е.А. Киршанова, Е.С. Малыгина, С.А. Новоселов, Д.О.Олефиренко. *Алгоритм нахождения образующих идеала Штикельбегера мультиквадратичных полей.* Prikl. Diskr. Mat., 2021, no. 51, 9–30 DOI `https://doi.org/10.17223/20710410/51/1`.

2. Elena Kirshanova, Thijs Laarhoven. *Lower Bounds on Lattice Sieving and Information Set Decoding.* CRYPTO (2) 2021: 791-820. DOI `10.1007/978-3-030-84245-1_27`

1.2 Результаты 2021 года

[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`

[3] Shweta Agrawal, Elena Kirshanova, Damien Stehlé, Anshu Yadav. *Can Round-Optimal Lattice-Based Blind Signatures be Practical?*. Статус: на рецензии. Полная версия доступна по адресу: `https://eprint.iacr.org/2021/1565`.

1.3 Обзор результатов

1. **Комбинаторые атаки на задачу NTRU**. Для некоторых $m \geq n \geq 1$ и $q \geq 2$, задача NTRU (известная также как тренарная задача LWE), просить отыскать по данным $(A, b = As + e \bmod q) \in (\mathbb{Z}/q\mathbb{Z})^{m \times n} \times (\mathbb{Z}/q\mathbb{Z})^m$, где матрица A состоит из случайных равномерно распределенных элементов из $\mathbb{Z}/q\mathbb{Z}$, неизвестные вектора $s \in \{-1, 0, 1\}^n$ и $e \in \{-1, 0, 1\}^m$. Можно полагать, что s, e также равномерно случайно распределены на своих областях определения. На трудности этой задачи основаны решетчатые криптосистемы семейства NTRU[1], а также некоторые схемы подписи на решетках.[2]

   В работе [1], 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.

   В другой работе [2], совместно с Alenxander May, мы улучшаем результаты его работы "How to meet ternary LWE keys", предлагая классический алгоритм решения третарной задачи LWE. Конкретнее, мы рассматриваем уравнение $b = As + e$ и разбиваем его на две части аналогично методу *встречи по-середине*: $As_1 + e_1 = b - As_2 - e_2$, где $s_1 \in \{-1, 0, 1\}^{n/2}||0^{n/2}$, $s_2 \in 0^{n/2}||\{-1, 0, 1\}^{n/2}$, $e_i \in \{0, 1\}^m$. Иначе говоря, мы имеем примерное равенство $As_1 \approx As_2 + b$. Мы не знаем s_1, s_2, но мы можем их перебрать. Оценка, корректна ли конкретная пара s_1, s_2, определяется алгоритмом поиска ближайшего соседа с помощью специальных, так называемых локально-чувствительных функций (locality-sensitive function). Мы предлагаем конкретную локально-чувствительную функцию и оцениваем сложность алгоритма для конкретных параметров тренарного LWE. Этот алгоритм имеет меньшую сложность, чем другие подходы решения задачи (например, алгоритмы редукции), в случаях, когда веса Хэмминга векторов ошибки секрета достаточно малы (меньше, чем $m/4$).

2. **Конструкции слепой подписи**. Слепая подпись – криптографический примитив, в которой пользователь $\mathcal{U}$, имеющий открытый ключ и сообщение, запрашивает у подписывающего $\mathcal{S}$, обладающего секретным ключом, подписать сообщение. При это подписывающий $\mathcal{S}$ не может сопоставить сообщению подпись, так как он подписывает зашифрованную версию сообщения. В свою очередь пользователь $\mathcal{U}$ не может подделать подпись, даже получая несколько (много) подписей от $\mathcal{S}$. Протокол слепой подписи используется а алгоритмах электронных денег, электронном голосовании, системах блокчейн. Например, в качестве пользователя $\mathcal{U}$ может быть покупатель какого-либо товара, запрашивающий у своего банка $\mathcal{S}$ подписать чек, то есть валидировать покупку. Банк при этом, не знает, что именно покупает его клиент $\mathcal{U}$, а клиент, в свою очередь, не может подделать подпись банка.

[1] Jeffrey Hoffstein, Jill Pipher, and Joseph H Silverman, Ntru: A ring-based public key cryptosystem, International Algorithmic Number Theory Symposium, 1998.

[2] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky, Lattice signatures and bimodal Gaussians, CRYPTO 2013.

В работе [3], мы предлагаем первую эффективную подпись, основанную на трудных задача на решетке. А именно, мы предлагаем конструкцию, основанную на версии задачи SIS (Sort Integer Solution). Задача определена как интерактивный протокол между двумя сторонами $\mathcal{C}$ и $\mathcal{A}$ и состоит в следующем:

- $\mathcal{C}$ выбирает случайным образом матрицу $C \in (\mathbb{Z}/q\mathbb{Z})^{n\times m}$ и отправляет её $\mathcal{A}$,
- $\mathcal{A}$ имеет возможность делать следующие запросы к $\mathcal{C}$:
  – запрос на получение синдрома, на который $\mathcal{C}$ выдает случайные вектор $t \in (\mathbb{Z}/q\mathbb{Z})^n$, – запрос на получение прообраза с входным вектором $t' \in (\mathbb{Z}/q\mathbb{Z})^n$, на который $\mathcal{C}$ выдает $y' \in (\mathbb{Z}/q\mathbb{Z})^m$, такой что $Cy' = t' \bmod q$ и евклидова норма y' мала.
- Сделав ℓ запросов на получение прообраза, $\mathcal{A}$ должен найти $\ell + 1$ различных пар $(t'_i, y'_i) \in (\mathbb{Z}/q\mathbb{Z})^n \times (\mathbb{Z}/q\mathbb{Z})^m$, таких что $Ct'_i = y'_i \bmod q$ и евклидовы нормы y'_i малы.

Моя задача в этой работе состояла в криптоанализе этой задачи. Я предлагаю два типа алгоритмов: комбинаторый алгоритм и алгоритм, основанный на редукции решетки. Для разных параметров m, n, q, ℓ разные типы алгоритмы работают быстрее.

3. Кроме вышеперечисленных статей, готовится к отправке в журнал обзорная статья “Quantum Algorithms to attack Hardness Assumptions in Post-Quantum Cryptography”, написанная совместно с Jean-Franǫis Biasse, Xavier Bonnetain, Martin M. Ekerå, André Schrottenloher, Fang Song.

2 Участие в конференциях и школах

1 `Тема:` Lower bounds on lattice sieving and information set decoding

`Место:` Third PQC Standardization Conference
`https://csrc.nist.gov/events/2021/third-pqc-standardization-conference` Вашинштон, США

`Дата:` 10.06.21

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

2 `Тема:` Lower bounds on lattice sieving and information set decoding

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

`Дата:` 15.05.21

`Слайды`
`https://simons.berkeley.edu/sites/default/files/docs/17620/elenakirshanovalatticesreu`
`pdf`

3 `Тема:` The SIS problem

`Место:` Семинар в Max Plank Institute, Саарбрюккен, Герамания

`Дата:` 26.07.21

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

4 Тема: Goppa Code in Classic McEliece

Место: Научный семинар в Рурском Университете г. Бохум, Германия

Дата: 20.09.21

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

5 Тема: Sidelnikov-Shestakov attack on Reed-Solomon code in McEliece

Место: Научный семинар в Рурском Университете г. Бохум, Германия

Дата: 30.11.21

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

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

3 Иная научная деятельность

- Программный комитет международных конференций
  – PQCrypto 2021 http://pqcrypto2021.kr/p_committee.php,
  – Crypto 2021 https://crypto.iacr.org/2021/callforpapers.php,
  – AsiaCrypt 2021 https://asiacrypt.iacr.org/2021/callforpapers.php,
  – PKC 2022 https://pkc.iacr.org/2022/callforpapers.php.
- Организатор летней школы "Workshop on Foundations and Applications of Lattice-based Cryptography", Эдинбург, Шотландия. Июль 2022.
  https://sites.google.com/view/lattice-research-workshop-2022/home
- Научный комитет, лектор, организатор летней школы "Aspects mathématiques de la cryptographie post-quantique". Рабат, Марокко. Октябрь 2023.
- Подготовка заявки на грант 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".

4 Педагогическая деятельность

- Научное руководство совместно с D.Stehlé над диссертацией Huyen Nguyen на тему "Cryptographic aspects of orthogonal lattices". Защита состоялась 15 ноября 2021 в ENS Lyon.
- Разработка и ведение нового курса "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_2021.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_2021.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 – Конкретная сложность алгоритмов декодирования для криптосистемы МакЭлиса (студентка Максимюк Е.В., дата зашиты 21.01.22)
  – Декодирование решеток с большим контактным числом (студент Гладкий Д.С., дата зашиты 21.01.22)

- Руководство аспирантом Карениным А.С. Тема диссертации “Алгоритмы нахождения короткого вектора в алгебраических решетках”.